(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2005 年8 月11 日 (11.08.2005)

PCT

(10) 国際公開番号
WO 2005/074187 A1

(51) 国際特許分類[7]: H04L 9/10, G06F 12/14, G09C 1/00, G11B 7/007, 7/30, 20/10, 20/12

(21) 国際出願番号: PCT/JP2005/001147

(22) 国際出願日: 2005 年1 月27 日 (27.01.2005)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2004-020827 2004 年1 月29 日 (29.01.2004) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒1410001 東京都品川区北品川６丁目７番３５号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 渡辺 綾子 (WATANABE, Ayako) [JP/JP]; 〒1410001 東京都品川区北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP). 高島 芳和 (TAKASHIMA, Yoshikazu) [JP/JP]; 〒1410001 東京都品川区北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP).

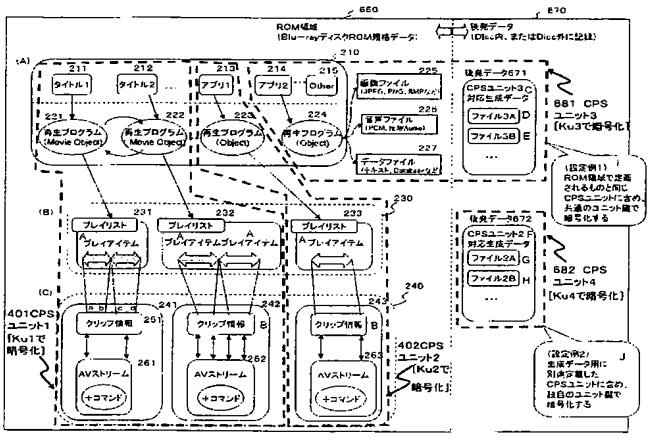
(74) 代理人: 宮田 正昭, 外(MIYATA, Masaaki et al.); 〒1040041 東京都中央区新富一丁目１番７号 銀座ティーケイビル 澤田・宮田・山田特許事務所 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE,

[続葉有]

(54) Title: INFORMATION PROCESSING DEVICE AND METHOD

(54) 発明の名称: 情報処理装置及び方法



660. ROM AREA (BLU-RAY DISC ROM SPECIFICATION DATA)
211 TITLE 1
212. TITLE 2
213. APPLICATION 1
214. APPLICATION 2
221. REPRODUCTION PROGRAM (MOVIE OBJECT)
222. REPRODUCTION PROGRAM (MOVIE OBJECT)
223. REPRODUCTION PROGRAM (OBJECT)
224. REPRODUCTION PROGRAM (OBJECT)
225. IMAGE FILE (JPEG, PNG, BMP, ETC.)
226. AUDIO FILE (PCM, COMPRESSED AUDIO)
227. DATA FILE (TEXT, DATABASE, ETC.)
231. PLAY LIST
232. PLAY LIST
233. PLAY LIST
A... PLAY ITEM
251. . CLIP INFORMATION
B... CLIP INFORMATION
261. . AV STREAM (+COMMAND)
262. . AV STREAM (+COMMAND)
263. . AV STREAM (+COMMAND)
401 CPS UNIT 1 [ENCRYPTED BY KU1]
402. . UNIT 2 [ENCRYPTED BY KU2]
670... LATER DATE (RECORDED IN DISC OR OUT OF DISC)
671... LATER DATA
C... DATA GENERATED CORRESPONDING TO CPS UNIT 3
D... FILE 3A
E... FILE 3B
672... LATE DATA
F DATA GENERATED CORRESPONDING TO CPS UNIT 2
G FILE 2A
H FILE 2B
681 CPS UNIT 3 [ENCRYPTED BY KU3]
I (SETTING EXAMPLE 1) INCLUDED IN THE SAME CPS UNIT AS DEFINED IN THE ROM AREA AND ENCRYPTED BY THE COMMON UNIT KEY
682. . CPS UNIT 4 [ENCRYPTED BY KU4]
J. (SETTING EXAMPLE 2) INCLUDED IN THE CPS UNIT DEFINED SEPARATELY FOR GENERATED DATA AND ENCRYPTED BY THE UNIQUE UNIT KEY

(57) Abstract: It is possible to provide use management for data generated or acquired after data which has been stored in an information recording medium, and secure data management. Late data such as information generated or downloaded later by a user in association with content information in the content management unit stored in an information recording medium is made into encrypted data by applying a unit key corresponding to a content management unit or a unit key corresponding to a new content management unit and recorded as data constituting the content management unit. With this configuration, it is possible to realize secure data management and use management of the late data like the original-unit-corresponding data.

[続葉有]

WO 2005/074187 A1

SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約: 情報記録媒体に格納済みデータと異なる後発的に生成または取得したデータについての利用管理、セキュアなデータ管理を可能とした構成を提供する。情報記録媒体に格納されたコンテンツ管理ユニット単位のコンテンツ情報に関連して後発的にユーザが生成した情報やダウンロードした情報などの後発データを、コンテンツ管理ユニットに対応するユニット鍵、または新規のコンテンツ管理ユニットに対応するユニット鍵を適用した暗号化データとして、コンテンツ管理ユニットの構成データとして記録する。本構成によれば、後発データについても、オリジナルのユニット対応データと同様のセキュアなデータ管理、利用管理が実現される。

明 細 書

次に示すように国際調査機関が作成した。
情報処理装置及び方法

[0001] 本発明は、情報処理装置、および情報処理方法、並びにコンピュータ・プログラムに関する。さらに、詳細には、情報記録媒体に格納されたユニット単位のコンテンツ情報に関連して後発的にユーザが生成した情報やダウンロードした情報などの後発データを、ユニットに対応する管理対象データとして記録し、後発生成データについてもユニット毎のセキュアなデータ管理および利用管理を実現する情報処理装置、および情報処理方法、並びにコンピュータ・プログラムに関する。

背景技術

[0002] 音楽等のオーディオデータ、映画等の画像データ、ゲームプログラム、各種アプリケーションプログラム等、様々なソフトウエアデータ(以下、これらをコンテンツ(Content)と呼ぶ)は、記録メディア、例えば、青色レーザを適用したBlu−rayディスク、あるいはDVD(Digital Versatile Disc)、MD(Mini Disc)、CD(Compact Disc)にデジタルデータとして格納することができる。特に、青色レーザを利用したBlu−rayディスクは、高密度記録可能なディスクであり大容量の映像コンテンツなどを高画質データとして記録することができる。

[0003] これら様々な情報記録媒体(記録メディア)にデジタルコンテンツが格納され、ユーザに提供される。ユーザは、所有するPC(Personal Computer)、ディスクプレーヤ等の再生装置においてコンテンツの再生、利用を行う。

[0004] 音楽データ、画像データ等、多くのコンテンツは、一般的にその作成者あるいは販売者に頒布権等が保有されている。従って、これらのコンテンツの配布に際しては、一定の利用制限、すなわち、正規なユーザに対してのみ、コンテンツの利用を許諾し、許可のない複製等が行われないようにする構成をとるのが一般的となっている。

[0005] デジタル記録装置および記録媒体によれば、例えば画像や音声を劣化させることなく記録、再生を繰り返すことが可能であり、不正コピーコンテンツのインターネットを介した配信や、コンテンツをCD−R等にコピーした、いわゆる海賊版ディスクの流通

や、PC等のハードディスクに格納したコピーコンテンツの利用が蔓延しているといった問題が発生している。

[0006] DVD、あるいは近年開発が進んでいる青色レーザを利用した記録媒体等の大容量型記録媒体は、1枚の媒体に例えば映画1本ー数本分の大量のデータをデジタル情報として記録することが可能である。このように映像情報等をデジタル情報として記録することが可能となってくると不正コピーを防止して著作権者の保護を図ることが益々重要な課題となっている。昨今では、このようなデジタルデータの不正なコピーを防ぐため、デジタル記録装置および記録媒体に違法なコピーを防止するための様々な技術が実用化されている。

[0007] 例えば、DVDプレーヤでは、コンテンツ・スクランブルシステム(Content Scramble System)が採用されている。コンテンツ・スクランブルシステムでは、DVD−ROM(Read Only Memory)に、ビデオデータやオーディオデータ等が暗号化されて記録されており、その暗号化されたデータを復号するのに用いる鍵が、ライセンスを受けたDVDプレーヤに与えられる。ライセンスは、不正コピーを行わない等の所定の動作規定に従うように設計されたDVDプレーヤに対して与えられる。従って、ライセンスを受けたDVDプレーヤでは、与えられたキーを利用して、DVD−ROMに記録された暗号化データを復号することにより、DVD−ROMから画像や音声を再生することができる。

[0008] 一方、ライセンスを受けていないDVDプレーヤは、暗号化されたデータを復号するための鍵を有していないため、DVD−ROMに記録された暗号化データの復号を行うことができない。このように、コンテンツ・スクランブルシステム構成では、ライセンス時に要求される条件を満たしていないDVDプレーヤは、デジタルデータを記録したDVD−ROMの再生を行なえないことになり、不正コピーが防止されるようになっている。

[0009] このように、情報記録媒体に格納されたコンテンツの管理システムは構築されている。しかし、例えば、情報記録媒体に格納されたコンテンツとしてのプログラムを実行してユーザが生成したデータや、外部サーバから取得したデータ、コンテンツなどについては、セキュアなデータ管理や、利用管理が実現されているとは言い難い。

[0010] ユーザが情報記録媒体に格納されたプログラムを実行して生成したデータや外部サーバから取得したデータについてセキュアな管理を行なう場合、例えばユーザが独自のパスワードを設定して保護したり、または、外部から取得した暗号鍵などを適用した暗号化データとするなど個別のデータ毎の対応が必要となる。このようなデータ管理構成をとると、生成データや取得データが増加した場合、管理すべき暗号鍵やパスワードが増大するという問題が発生し、また、データの所在が不明確になりやすく、さらに格納データと暗号鍵／パスワードとの対応についても不明確になってしまうといった問題がある。また、このような後発データについての利用管理についても十分な対策がとられていないという現状がある。

発明の開示

発明が解決しようとする課題

[0011] 本発明は、このような状況に鑑みてなされたものであり、情報記録媒体に格納されたユニット単位のコンテンツ情報に関連して後発的にユーザが生成した情報やダウンロードした情報などの後発データを、ユニットに対応の管理データとして記録し、後発生成データについてもユニット毎のセキュアなデータ管理および利用管理を実現する情報処理装置、および情報処理方法、並びにコンピュータ・プログラムを提供することを目的とするものである。

課題を解決するための手段

[0012] 本発明の第1の側面は、

情報処理装置であり、

情報記録媒体からのデータ読み取りを実行する記録媒体インタフェースと、

前記情報記録媒体からの取得情報を適用して生成または取得した後発データの記録処理を実行するデータ処理部を有し、

前記情報記録媒体は、各々が異なる暗号鍵として設定されるユニット鍵による暗号化データを含むコンテンツ管理ユニット単位の記録データを格納した情報記録媒体であり、

前記データ処理部は、

前記取得情報の属するコンテンツ管理ユニットに対応するユニット鍵、または新規

のコンテンツ管理ユニットに対応するユニット鍵を取得して、取得ユニット鍵を適用した前記後発データの暗号化処理を実行し、生成した暗号化データをコンテンツ管理ユニットの構成データとして記録する処理を実行する構成であることを特徴とする情報処理装置にある。

[0013] さらに、本発明の情報処理装置の一実施態様において、前記データ処理部は、前記後発データに対応するコンテンツ管理ユニットを設定するとともに、該後発データを含むコンテンツ管理ユニットに対応する管理情報としての暗号鍵の設定処理を実行する構成であることを特徴とする。

[0014] さらに、本発明の情報処理装置の一実施態様において、前記データ処理部は、前記後発データに対応するコンテンツ管理ユニットを設定するとともに、該後発データを含むコンテンツ管理ユニットに対応する管理情報としてのコンテンツ利用制御情報の設定処理を実行する構成であることを特徴とする。

[0015] さらに、本発明の情報処理装置の一実施態様において、前記データ処理部は、前記情報記録媒体からの取得情報に含まれるプログラムによって規定された領域に対して、前記後発データの書き込み処理を実行する構成であることを特徴とする。

[0016] さらに、本発明の情報処理装置の一実施態様において、前記データ処理部は、前記取得情報を取得した情報記録媒体以外の記憶手段に前記後発データを格納する場合において、前記取得情報を取得した情報記録媒体の識別情報を該後発データに対応付けて格納する処理を実行する構成であることを特徴とする。

[0017] さらに、本発明の情報処理装置の一実施態様において、前記データ処理部は、後発データを含むAVストリームデータファイル、およびAVストリームデータの再生処理に適用する制御情報またはプログラムを含むナビケーションファイルの暗号化処理を実行して、記憶手段に対する後発データの記録処理を実行する構成であることを特徴とする。

[0018] さらに、本発明の情報処理装置の一実施態様において、前記データ処理部は、前記暗号化処理に適用する暗号鍵として、コンテンツ管理ユニットに対応するユニット鍵を適用する構成であることを特徴とする。

[0019] さらに、本発明の情報処理装置の一実施態様において、前記データ処理部は、前

記コンテンツ管理ユニットに対する処理を実行するライセンスされたアプリケーションによってのみ取得可能な情報を暗号鍵または暗号鍵生成情報として適用した暗号化処理を実行する構成であることを特徴とする。

[0020] さらに、本発明の情報処理装置の一実施態様において、前記ライセンスされたアプリケーションによってのみ取得可能な情報は、前記アプリケーションのインストールされたデバイスに固有の識別子としてのデバイスIDを含む情報であることを特徴とする。

[0021] さらに、本発明の情報処理装置の一実施態様において、前記データ処理部は、後発データを含むAVストリームデータファイル、およびAVストリームデータの再生処理に適用する制御情報またはプログラムを含むナビケーションファイルの少なくともいずれかのファイルに対して、改竄検証のためのハッシュ値を生成して記憶手段に記録する処理を実行する構成であることを特徴とする。

[0022] さらに、本発明の情報処理装置の一実施態様において、前記データ処理部は、後発データを含むAVストリームデータファイルまたはナビケーションファイルの利用に際して、ファイルに対して設定されたハッシュ値に基づくデータ改竄検証処理を実行し、改竄のないことの確認を条件として各ファイルの利用処理を実行する構成であることを特徴とする。

[0023] さらに、本発明の情報処理装置の一実施態様において、前記データ処理部は、後発データを含むAVストリームデータの再生処理に適用する制御情報またはプログラムを含むナビケーションファイルを、改竄検証のための電子署名を付加したファイルとして記憶手段に記録する処理を実行する構成であることを特徴とする。

[0024] さらに、本発明の情報処理装置の一実施態様において、前記データ処理部は、後発データを含むAVストリームデータファイルまたはビケーションファイルの利用に際して、ファイルに対して設定された電子署名に基づくデータ改竄検証処理を実行し、改竄のないことの確認を条件として各ファイルの利用処理を実行する構成であることを特徴とする。

[0025] さらに、本発明の第2の側面は、

情報処理装置であり、

情報記録媒体からのデータ読み取りを実行する記録媒体インタフェースと、

前記情報記録媒体からの読み取り情報に含まれるプログラムの処理を行なうデータ処理部を有し、

前記データ処理部は、

プログラムを読み取った情報記録媒体の種類を判定し、予め設定されたプログラム実行の許容された種類であることの確認を条件としてプログラムを実行する構成であることを特徴とする情報処理装置にある。

[0026] さらに、本発明の情報処理装置の一実施態様において、前記データ処理部は、プログラム実行の許可される情報記録媒体の種類情報を、前記情報記録媒体からの読み取り情報から取得し、該取得情報に従ってプログラムの実行可否判定を行なう構成であることを特徴とする。

[0027] さらに、本発明の第3の側面は、

情報処理方法であり、

情報記録媒体からのデータ読み取りを実行するデータ読み取りステップと、

前記情報記録媒体からの取得情報を適用して生成または取得した後発データの記録処理を実行するデータ処理ステップを有し、

前記情報記録媒体は、各々が異なる暗号鍵として設定されるユニット鍵による暗号化データを含むコンテンツ管理ユニット単位の記録データを格納した情報記録媒体であり、

前記データ処理ステップは、

前記取得情報の属するコンテンツ管理ユニットに対応するユニット鍵、または新規のコンテンツ管理ユニットに対応するユニット鍵を取得するステップと、

取得ユニット鍵を適用した前記後発データの暗号化処理を実行するステップと、

生成した暗号化データをコンテンツ管理ユニットの構成データとして記録する処理を実行するステップと、

を含むことを特徴とする情報処理方法にある。

[0028] さらに、本発明の情報処理方法の一実施態様において、前記データ処理ステップは、前記後発データに対応するコンテンツ管理ユニットを設定するとともに、該後発

データを含むコンテンツ管理ユニットに対応する管理情報としての暗号鍵の設定処理を実行するステップを含むことを特徴とする。

[0029] さらに、本発明の情報処理方法の一実施態様において、前記データ処理ステップは、前記後発データに対応するコンテンツ管理ユニットを設定するとともに、該後発データを含むコンテンツ管理ユニットに対応する管理情報としてのコンテンツ利用制御情報の設定処理を実行するステップを含むことを特徴とする。

[0030] さらに、本発明の情報処理方法の一実施態様において、前記データ処理ステップは、前記情報記録媒体からの取得情報に含まれるプログラムによって規定された領域に対して、前記後発データの書き込み処理を実行するステップを含むことを特徴とする。

[0031] さらに、本発明の情報処理方法の一実施態様において、前記データ処理ステップは、前記取得情報を取得した情報記録媒体以外の記憶手段に前記後発データを格納する場合において、前記取得情報を取得した情報記録媒体の識別情報を該後発データに対応付けて格納する処理を実行することを特徴とする。

[0032] さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、さらに、後発データを含むAVストリームデータファイル、およびAVストリームデータの再生処理に適用する制御情報またはプログラムを含むナビケーションファイルの暗号化処理を実行して、記憶手段に記録する処理を実行する暗号化記録処理ステップを含むことを特徴とする。

[0033] さらに、本発明の情報処理方法の一実施態様において、前記暗号化記録処理ステップは、コンテンツ管理ユニットに対応するユニット鍵を暗号鍵として適用した暗号化処理を実行するステップであることを特徴とする。

[0034] さらに、本発明の情報処理方法の一実施態様において、前記暗号化記録処理ステップは、前記コンテンツ管理ユニットに対する処理を実行するライセンスされたアプリケーションによってのみ取得可能な情報を暗号鍵または暗号鍵生成情報として適用した暗号化処理を実行するステップであることを特徴とする。

[0035] さらに、本発明の情報処理方法の一実施態様において、前記ライセンスされたアプリケーションによってのみ取得可能な情報は、前記アプリケーションのインストールさ

れたデバイスに固有の識別子としてのデバイスIDを含む情報であることを特徴とする。

[0036] さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、さらに、後発データを含むAVストリームデータファイル、およびAVストリームデータの再生処理に適用する制御情報またはプログラムを含むナビケーションファイルの少なくともいずれかのファイルに対して、改竄検証のためのハッシュ値を生成して記憶手段に記録する処理を実行するステップを有することを特徴とする。

[0037] さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、さらに、後発データを含むAVストリームデータファイルまたはナビケーションファイルの利用に際して、ファイルに対して設定されたハッシュ値に基づくデータ改竄検証処理を実行し、改竄のないことの確認を条件として各ファイルの利用処理を実行するステップを有することを特徴とする。

[0038] さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、さらに、後発データを含むAVストリームデータの再生処理に適用する制御情報またはプログラムを含むナビケーションファイルを、改竄検証のための電子署名を付加したファイルとして記憶手段に記録する処理を実行するステップを有することを特徴とする。

[0039] さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、さらに、後発データを含むAVストリームデータファイルまたはビケーションファイルの利用に際して、ファイルに対して設定された電子署名に基づくデータ改竄検証処理を実行し、改竄のないことの確認を条件として各ファイルの利用処理を実行するステップを有することを特徴とする。

[0040] さらに、本発明の第4の側面は、

情報処理方法であり、

情報記録媒体からのデータ読み取りを実行するデータ読み取りステップと、

前記情報記録媒体からの読み取り情報に含まれるプログラムの処理を行なうデータ処理ステップを有し、

前記データ処理ステップは、

プログラムを読み取った情報記録媒体の種類を判定し、予め設定されたプログラム実行の許容された種類であることの確認を条件としてプログラムを実行するステップを含むことを特徴とする情報処理方法にある。

[0041] さらに、本発明の情報処理方法の一実施態様において、前記データ処理ステップにおいて、プログラム実行の許可される情報記録媒体の種類情報を、前記情報記録媒体からの読み取り情報から取得し、該取得情報に従ってプログラムの実行可否判定を行なうことを特徴とする。

[0042] さらに、本発明の第5の側面は、

情報処理を実行するコンピュータ・プログラムであり、

情報記録媒体からのデータ読み取りを実行するデータ読み取りステップと、

前記情報記録媒体からの取得情報を適用して生成または取得した後発データの記録処理を実行するデータ処理ステップを有し、

前記情報記録媒体は、各々が異なる暗号鍵として設定されるユニット鍵による暗号化データを含むコンテンツ管理ユニット単位の記録データを格納した情報記録媒体であり、

前記データ処理ステップは、

前記取得情報の属するコンテンツ管理ユニットに対応するユニット鍵、または新規のコンテンツ管理ユニットに対応するユニット鍵を取得するステップと、

取得ユニット鍵を適用した前記後発データの暗号化処理を実行するステップと、

生成した暗号化データをコンテンツ管理ユニットの構成データとして記録する処理を実行するステップと、

を含むことを特徴とするコンピュータ・プログラムにある。

[0043] さらに、本発明のコンピュータ・プログラムの一実施態様において、前記コンピュータ・プログラムは、さらに、後発データを含むAVストリームデータファイル、およびAVストリームデータの再生処理に適用する制御情報またはプログラムを含むナビケーションファイルの暗号化処理を実行して記憶手段に記録する処理を実行する暗号化記録処理ステップを有することを特徴とする。

[0044] さらに、本発明のコンピュータ・プログラムの一実施態様において、前記コンピュー

タ・プログラムは、さらに、後発データを含むAVストリームデータファイル、およびAVストリームデータの再生処理に適用する制御情報またはプログラムを含むナビケーションファイルの少なくともいずれかのファイルに対する改竄検証用データを記憶手段に記録する処理を実行するステップを有することを特徴とする。

[0045] さらに、本発明のコンピュータ・プログラムの一実施態様において、前記コンピュータ・プログラムは、さらに、後発データを含むAVストリームデータファイルまたはナビケーションファイルの利用に際して、ファイルに対して設定された改竄検証用データに基づくデータ改竄検証処理を実行し、改竄のないことの確認を条件として各ファイルの利用処理を実行するステップを有することを特徴とする。

[0046] さらに、本発明の第6の側面は、

情報処理を実行するコンピュータ・プログラムであり、

情報記録媒体からのデータ読み取りを実行するデータ読み取りステップと、

前記情報記録媒体からの読み取り情報に含まれるプログラムの処理を行なうデータ処理ステップを有し、

前記データ処理ステップは、

プログラムを読み取った情報記録媒体の種類を判定し、予め設定されたプログラム実行の許容された種類であることの確認を条件としてプログラムを実行するステップを含むことを特徴とするコンピュータ・プログラムにある。

[0047] なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能なコンピュータ・システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体、例えば、DVD、CD、MOなどの記録媒体、あるいは、ネットワークなどの通信媒体によって提供可能なコンピュータ・プログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、コンピュータ・システム上でプログラムに応じた処理が実現される。

[0048] 本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

発明の効果

[0049] 本発明の構成によれば、情報記録媒体に格納されたコンテンツ管理ユニット単位のコンテンツ情報に関連して後発的にユーザが生成した情報やダウンロードした情報などの後発データを、コンテンツ管理ユニットに対応するユニット鍵、または新規のコンテンツ管理ユニットに対応するユニット鍵を適用した暗号化データとして、コンテンツ管理ユニットの構成データとして記録する構成としたので、後発生成データについてもオリジナルのユニット対応データと同様のセキュアなデータ管理、利用管理が実現される。

[0050] さらに、本発明の構成によれば、情報記録媒体からの読み取り情報に含まれるプログラムの実行において、プログラムを読み取った情報記録媒体の種類を判定し、予め設定されたプログラム実行の許容された種類であることの確認を条件としてプログラムを実行する構成としたので、例えばコンテンツのコピーディスクを利用したプログラム実行が拒否されることとなり、コンテンツの不正利用を防止することが可能となる。

[0051] さらに、本発明の構成によれば、AVストリームデータファイル以外のナビケーションファイルについても暗号化または改竄検証用データを設定して格納する構成としたので、例えば、PCなど様々なアプリケーションソフトが利用可能な装置において、ライセンスされたアプリケーション以外のアプリケーションを適用してCPSユニット対応のAVストリームデータファイルやナビケーションファイルを利用したり、データ変更を行なうなどの処理を防止することが可能となり、ナビケーションファイルを含むCPSユニット対応データの不正利用の排除が可能となる。

図面の簡単な説明

[0052] [図1]情報記録媒体の格納データ構成について説明する図である。

[図2]CPSユニット管理テーブルの例を示す図である。

[図3]情報記録媒体の格納コンテンツに対して設定するコンテンツ管理ユニットの設定例について説明する図である。

[図4]情報記録媒体の格納コンテンツに対して設定するコンテンツ管理ユニットの暗号化構成例について説明する図である。

[図5]情報記録媒体におけるデータ格納ディレクトリの構成例について説明する図

である。

[図6]情報記録媒体を装着した情報処理装置における後発データの生成または取得処理について説明する図である。

[図7]情報処理装置における後発データの取得処理シーケンスについて説明する図である。

[図8]情報処理装置において生成または取得する後発データの例について説明する図である。

[図9]情報処理装置において生成または取得する後発データの例について説明する図である。

[図10]情報処理装置において生成または取得した後発データとCPSユニットとの関係について説明する図である。

[図11]情報処理装置において生成または取得した後発データの再生／コピー制御情報の設定例について説明する図である。

[図12]情報処理装置において生成または取得した後発データの暗号鍵情報の設定例について説明する図である。

[図13]ナビケーションファイルの暗号化格納処理構成について説明する図である。

[図14]ナビケーションファイルの改竄を防止し、改竄の検証を可能とした格納処理構成について説明する図である。

[図15]情報処理装置において生成または取得した後発データの書き込み処理シーケンスについて説明するフロー図である。

[図16]情報処理装置において生成または取得した後発データについてCPSユニットとして識別する構成について説明する図である。

[図17]情報処理装置において生成または取得した後発データについてCPSユニットとして識別し取得するための構成について説明する図である。

[図18]情報処理装置において生成または取得した後発データについてCPSユニットとして識別する構成について説明する図である。

[図19]プログラムの実行を情報記録媒体の種別に基づいて制限する処理シーケンスについて説明するフロー図である。

[図20]プログラムの実行を情報記録媒体の種別に基づいて制限する処理の具体例について説明する図である。

[図21]情報記録媒体を装着して再生処理または記録処理を実行する情報処理装置の構成例について説明する図である。

発明を実施するための最良の形態

[0053] 以下、図面を参照しながら本発明の情報処理装置、および情報処理方法、並びにコンピュータ・プログラムの詳細について説明する。なお、説明は、以下の記載項目に従って行う。

1. 情報記録媒体の格納データ
2. コンテンツ格納構成
3. 格納コンテンツの暗号化、利用管理構成
4. 後発的に生成したデータまたは取得したデータの管理構成
5. ナビゲーションファイルの暗号化および改竄防止構成
6. 情報処理装置が生成または取得した後発データの格納処理
7. 情報記録媒体のCPSユニット構成データと情報記録媒体外部に格納したCPSユニット構成データの関連づけ構成
8. プログラム実行条件を限定した処理構成
9. 情報処理装置の構成例

[0054] [1. 情報記録媒体の格納データ]

まず、情報記録媒体の格納データについて説明する。図1に、本発明の処理の適用可能なコンテンツの格納された情報記録媒体の一例を示す。

[0055] 情報記録媒体100は、正当なコンテンツ著作権、あるいは頒布権を持ついわゆるコンテンツ権利者の許可の下にディスク製造工場において製造された正当なコンテンツを格納した情報記録媒体である。なお、以下の実施例では、情報記録媒体の例としてディスク型の媒体を例として説明するが、本発明は様々な態様の情報記録媒体を用いた構成において適用可能である。

[0056] 情報記録媒体100は、例えばデータ再書き込みの不可能なROMディスク、あるいは、一部分のデータ領域のみデータ書き込み可能なパーシャルROM(Partial RO

M)ディスク、あるいは全領域においてデータ書き込み可能なディスクなど、様々な態様の記録媒体である。

[0057] 図1に示すように、情報記録媒体100にはコンテンツ101が格納される。例えば高精細動画像データであるHD(High Definition)ムービーコンテンツなどの動画コンテンツのAV(Audio Visual)ストリームや特定の規格で規定された形式のゲームプログラム、画像ファイル、音声データ、テキストデータなどからなるコンテンツ101である。これらのコンテンツには、情報記録媒体100からのデータのみによって利用可能な情報、あるいは情報記録媒体100からのデータと、ネットワーク接続されたサーバから提供されるデータとを併せて利用可能となる情報など、様々な態様の情報が含まれる。

[0058] 情報記録媒体100に格納されるコンテンツ101は、少なくとも一部が暗号化コンテンツとして格納されており、暗号化コンテンツの復号処理に適用する鍵の生成に必要となる情報として記録シード(REC SEED)102が格納される。暗号化コンテンツは、コンテンツの利用管理のため、各々、個別の暗号鍵としてのユニット鍵を適用した暗号化データとして情報記録媒体100に格納される。記録シード(REC SEED):Vu102は、個別のユニット鍵の生成のために適用する鍵生成情報である。なお、記録シード(REC SEED)102は情報記録媒体100に格納される設定のみならず、例えばネットワーク接続されたサーバから取得する設定としてもよい。

[0059] 情報記録媒体100には、さらに、情報記録媒体100の識別情報としてのディスクID103、情報記録媒体100の格納コンテンツの編集スタジオの識別子としてのスタジオID104、情報記録媒体100の製造単位としてのパッケージ識別子としてのパッケージID105、ディスク種別識別情報106が格納される。

[0060] 情報記録媒体100に格納されるコンテンツは、例えば高精細動画像データであるHD(High Definition)ムービーコンテンツなどの動画コンテンツのAV(Audio Visual)ストリームや特定の規格で規定された形式のゲームプログラム、画像ファイル、音声データ、テキストデータなどからなるコンテンツである。例えば情報記録媒体が、高密度記録可能な青色レーザによるデータ記録ディスクであるBlu-rayディスクの場合には、Blu-rayディスクROM規格フォーマットに従ったデータがメインコンテンツとして

格納される。

[0061] さらに、例えばサービスデータとしてのゲームプログラムや、画像ファイル、音声データ、テキストデータなどのコンテンツなど、特定のAVデータフォーマットに従わないデータフォーマットを持つデータをサブコンテンツとして格納する場合もある。

[0062] 情報記録媒体100に格納される様々なコンテンツ101は、コンテンツの利用管理のため、各々、個別のユニット鍵を適用した暗号化がなされて情報記録媒体100に格納される。ユニット鍵を生成する鍵生成情報として記録シード102が適用される。

[0063] すなわち、コンテンツを構成するAV(Audio Visual)ストリーム、音楽データ、動画、静止画等の画像データ、ゲームプログラム、WEBコンテンツなどは、コンテンツ利用の管理単位としてのユニットに区分され、区分されたユニット毎に異なる記録シード:Vu102が割り当てられ、それぞれのユニットに対応する記録シードに基づいてユニット鍵が生成可能であり、ユニット鍵を適用した暗号化コンテンツの復号処理によって再生が可能となる。

[0064] 例えば、情報記録媒体100に格納されるAV(Audio Visual)ストリームのコンテンツ利用に際しては、記録シード:Vu102と、図には示していないが、情報記録媒体100に記録された物理インデックスなどその他の秘密情報を適用した所定の暗号鍵生成シーケンスを実行してユニット対応のユニット鍵を取得して、取得したユニット鍵に基づいてユニットに含まれる暗号化コンテンツの復号処理を行ない再生する。

[0065] 上述したように、情報記録媒体100に格納される暗号化コンテンツは、コンテンツ利用管理単位としてのユニットに区分されている。このユニットをCPSユニット(コンテンツ管理ユニット)と呼ぶ。CPSユニット構成および記録シードの対応例を図2に示す。図2には、情報記録媒体に格納されるコンテンツ管理情報としてのCPSユニット管理テーブルと、各ユニット対応の記録シードに基づいて生成可能なCPSユニット鍵の対応を示している。

[0066] 図2のCPSユニット管理テーブルに示すように、CPSユニットの設定単位は、コンテンツのタイトル、アプリケーション、データグループなど、様々であり、CPSユニット管理テーブルには、それぞれのCPSユニットに対応する識別子としてのCPSユニットIDと、記録シード情報が対応付けられて設定される。

[0067] 図2において、タイトル1はCPSユニット1であり記録シードとしてVu1が対応して設定され、タイトル2はCPSユニット1であり記録シードとしてVu1が対応して設定され、アプリケーション1はCPSユニット2として設定されている。

[0068] 例えば、記録シードVu1に基づいて、ユニット鍵Ku1が生成され、ユニット鍵Ku1を適用した暗号処理によって、タイトル1とタイトル2によって判別可能な1つのCPSユニット(CPS1)に含まれる暗号化コンテンツの復号処理が可能となる。同様に、記録シードVu2に基づいて、ユニット鍵Ku2が生成され、ユニット鍵Ku2を適用した暗号処理によって、アプリケーション1によって判別可能な1つのCPSユニット(CPS2)に含まれる暗号化コンテンツの復号処理が可能となる。以下、同様である。

[0069] なお、CPSユニット管理テーブルには、情報記録媒体に格納されているコンテンツ以外の、例えばユーザが後発的に生成したデータや外部から取得したデータなどの後発データのためのCPSユニットが設定されている。これらは、後発データに対してユーザが新規に定義可能なCPSユニットである。図2に示すデータフィールド121に対応するCPSユニットが後発データ用のユニットとして適用可能である。

[0070] このCPSユニットは、情報記録媒体に格納されているコンテンツ、例えばプログラムの実行によって取得したデータ、具体的にはゲームの途中経過情報、得点情報などの後発的に生成されるデータや、情報記録媒体に格納されているコンテンツであるAVストリームに対応する付属データ、例えば外部サーバから取得した字幕データなど、ユーザが生成または取得した後発データに対する管理ユニットとして設定可能なユニットである。これらの利用形態については、後段で詳細に説明する。

[0071] [2. コンテンツ格納構成]

図3を参照して、本発明の情報記録媒体に格納されるコンテンツの格納フォーマットについて説明する。

[0072] 情報記録媒体には、図3に示すように、例えば高精細動画像データであるHD(High Definition)ムービーコンテンツなどの動画コンテンツのAVストリームをメインコンテンツ200として格納し、その他のデータ、プログラム、例えばサービスデータとしてのゲームプログラムや、画像ファイル、音声データ、テキストデータなどがサブコンテンツ300として格納されている。

[0073] メインコンテンツ200は、特定のAVフォーマット、例えばBlu-rayディスクROM規格データとして、Blu-rayディスクフォーマットに従って格納され、サブコンテンツ300は、Blu-rayディスクフォーマット外データとして、Blu-rayディスクフォーマットに従わない任意のフォーマットで格納される。

[0074] 図3に示すように、Blu-rayディスクフォーマットに従って格納されるメインコンテンツ200は、動画コンテンツ(AVストリーム)を再生対象の実コンテンツとして格納しており、Blu-rayディスクフォーマットに従った階層構成を持つ。すなわち、

(A)アプリケーション210

(B)再生区間指定ファイル(プレイリスト)230

(C)クリップ(コンテンツデータファイル)240

である。

[0075] (C)クリップ(コンテンツデータファイル)240は、それぞれ区分されたコンテンツデータファイルであるクリップ241, 242, 243を有し、各クリップ241は、AV(Audio-Visual)ストリームファイル261とクリップ情報ファイル251を持つ。

[0076] クリップ情報ファイル251は、AV(Audio-Visual)ストリームファイル261に関する属性情報を格納したデータファイルである。AV(Audio-Visual)ストリームファイル261は例えばMPEG-TS(Moving Picture Experts Group-Transport Stream)データであり、画像(Video)、音声(Audio)、字幕データ等の各情報を多重化したデータ構造となっている。また、再生時に再生装置の制御を行うためのコマンド情報も多重化されている場合がある。

[0077] (B)再生区間指定ファイル(プレイリスト)230は、複数の再生区間指定ファイル(プレイリスト)231, 232, 233を持つ。各再生区間指定ファイル(プレイリスト)231, 232, 233のそれぞれは、クリップ(コンテンツデータファイル)240に含まれる複数のAVストリームデータファイルのいずれかを選択し、また選択したAVストリームデータファイルの特定のデータ部分を、再生開始点と再生終了点として指定するプレイアイテムを1つ以上持つ構成となっており、1つの再生区間指定ファイル(プレイリスト)を選択することで、その再生区間指定ファイル(プレイリスト)の持つプレイアイテムに従って、

再生シーケンスが決定されて再生が実行される。

[0078] 例えば再生区間指定ファイル(プレイリスト)231を選択してコンテンツ再生を行うと、再生区間指定ファイル(プレイリスト)231に対応付けられたプレイアイテム234は、クリップ241に再生開始点aと再生終了点bを持ち、また、プレイアイテム235は、クリップ241に再生開始点cと再生終了点dを持つので、再生区間指定ファイル(プレイリスト)231を選択してコンテンツ再生を行うと、クリップ241に含まれるコンテンツであるAVストリームファイル261の特定データ領域、a一bとc一dが再生されることになる。

[0079] (A)アプリケーション210は、たとえばコンテンツ再生を実行するディスプレイに提示されるコンテンツタイトルを含むアプリケーションインデックスファイル211, 212と再生プログラム221, 222の組み合わせ、または、ゲームコンテンツ、WEBコンテンツなどのアプリケーション実行ファイル213, 214と再生プログラム223, 224の組み合わせを持つ層として設定される。ユーザは再生対象をアプリケーションインデックスファイル211, 212に含まれるタイトルの選択によって決定することができる

[0080] 各タイトルは、図に示すように、再生プログラム221一224の1つの再生プログラム(例えばムービーオブジェクト)に対応付けられており、ユーザが1つのタイトルを選択すると、その選択したタイトルに対応付けられた再生プログラムに基づく再生処理が開始することになる。なお、図に示すタイトル1、タイトル2として示されるアプリケーションインデックスファイル211, 212は、情報記録媒体のセット、起動に際して、自動的に再生されるタイトル、メニューを表示するためのタイトル提示プログラムも含まれる。

[0081] アプリケーションインデックスファイル211, 212や、アプリケーション実行ファイル213, 214は、アプリケーション実行に使用されるアプリケーションリソースファイルを含む場合がある。また、情報記録媒体、あるいはネットワーク接続サーバから取得可能な様々なデータファイル、例えばJPEG, PNG, BMPなどの画像ファイル225、PCM、圧縮Audioなどの音声ファイル226、テキスト、データベースなどの各種データファイル227がアプリケーションリソースファイルとして適用される場合もある。

[0082] 再生プログラム(例えばムービーオブジェクト)221一224は、再生する再生区間指定ファイル(プレイリスト)の指定のほか、ユーザから入力されるコンテンツ再生処理に関する操作情報に対する応答、タイトル間のジャンプ、再生シーケンスの分岐など、

再生コンテンツ(HDムービーコンテンツ)の提示に必要な機能をプログラマブルに提供するコンテンツ再生処理プログラムである。各再生プログラム221ー224は、相互にジャンプ可能であり、ユーザの入力、あるいはあらかじめ設定されたプログラムに従って、実際に実行される再生プログラムが選択され、選択された再生プログラムの指定する再生区間指定ファイル(プレイリスト)230によって、再生コンテンツがクリップ240から選択され再生される。

[0083] メインコンテンツ200は、図に示すように、例えばBlu-rayディスクROM規格データとして、Blu-rayディスクROM規格フォーマットに従った階層構成で管理され、この階層構成の枠組みに対して、コンテンツ管理ユニット(CPSユニット)が設定され、コンテンツ管理ユニット(CPSユニット)単位でコンテンツの利用管理がなされる。コンテンツ管理ユニット(CPSユニット)についての詳細は後述する。

[0084] 情報記録媒体には、メインコンテンツ200の他にサブコンテンツ300が併せて格納される。サブコンテンツ300は、特定のAVフォーマット、例えばBlu-rayディスクROM規格フォーマットに従わない任意のフォーマットで格納されるコンテンツである。

[0085] サブコンテンツ300は、例えばサービスデータとしてのゲームプログラムや、画像ファイル、音声データ、テキストデータなどであり、複数のデータファイルからなる集合がデータグループとして設定される。

[0086] 図3にはデータグループ1, 311ーデータグループN, 312を示している。これらのデータグループも利用管理対象コンテンツとして設定可能であり、利用管理対象コンテンツとして設定した場合には、各データグループを単位としたコンテンツ管理ユニット(CPSユニット)が設定され、データグループ単位で利用管理がなされる。

[0087] [3. 格納コンテンツの暗号化、利用管理構成]

次に、図4以下を参照して、情報記録媒体に格納されたコンテンツをコンテンツ管理ユニット(CPSユニット)に区分して、各ユニット毎に異なる利用制御を実現するコンテンツ管理構成について説明する。

[0088] 先に図2を参照して説明したように、コンテンツ管理ユニット(CPSユニット)の各々に対して、異なる暗号鍵としてユニット鍵が割り当てられる。1つのユニット鍵を割り当てる単位がコンテンツ管理ユニット(CPSユニット)である。なお、ユニット鍵は、ユニッ

トに対応する記録シードに基づいて生成可能な鍵である。

[0089] それぞれのユニット鍵を適用して各ユニットに属するコンテンツを暗号化し、コンテンツ利用に際しては、各ユニットに割り当てられたユニット鍵を取得して再生を行う。各ユニット鍵は、個別に管理することが可能であり、例えばあるユニットAに対して割り当てるユニット鍵は、情報記録媒体から取得可能な鍵として設定する。また、ユニットBに対して割り当てるユニット鍵は、ネットワーク接続されるサーバにアクセスし、ユーザが所定の手続きを実行したことを条件として取得することができる鍵とするなど、各ユニット対応の鍵の取得、管理構成は、各ユニット鍵に独立した態様とすることが可能である。

[0090] 1つの鍵を割り当てる単位、すなわち、コンテンツ管理ユニット(CPSユニット)の設定態様について、図4を参照して説明する。

[0091] まず、メインコンテンツ200側におけるコンテンツ管理ユニット(CPSユニット)の設定構成について説明する。

[0092] メインコンテンツ200側においては、(A)アプリケーション210に含まれる1つ以上のタイトルを含むアプリケーションインデックスファイル211, 212、またはアプリケーション実行ファイル213, 214等を含むCPSユニットを設定する。

[0093] 図4に示すCPSユニット1, 401は、アプリケーションインデックスファイルと、再生プログラムファイルと、プレイリストと、コンテンツ実データとしてのAVストリームファイル群とを1つのユニットとして設定したユニットである。

[0094] また、CPSユニット2, 402は、アプリケーション実行ファイルと、再生プログラムファイルと、プレイリストと、コンテンツ実データとしてのAVストリームファイル群とを1つのユニットとして設定したユニットである。

[0095] また、CPSユニット3, 403は、アプリケーション実行ファイルと、再生プログラムファイルと、情報記録媒体、あるいはネットワーク接続サーバから取得可能な様々なデータファイルによって構成したユニットである。

[0096] これらの各ユニットは、同一の鍵(CPSユニット鍵:図4中の鍵Ku1, Ku2, Ku3)でそれぞれ個別に暗号化して情報記録媒体に格納される。

[0097] 図4中、コンテンツ管理ユニット(CPSユニット)1, 401、およびコンテンツ管理ユニ

ット(CPSユニット)2, 402は、上位層の(A)アプリケーションと、下位層の(B)再生区間指定ファイル(プレイリスト)＋(C)クリップ(コンテンツデータファイル)によって構成されるユニットであり、コンテンツ管理ユニット(CPSユニット)3, 403は、下位層の(B)再生区間指定ファイル(プレイリスト)＋(C)クリップ(コンテンツデータファイル)を含まず、上位層の(A)アプリケーション層、および情報記録媒体、あるいはネットワーク接続サーバから取得可能な様々なデータファイルすなわち、画像ファイル225、音声ファイル226、データファイル227等によって構成されるユニットである。

[0098] コンテンツ管理ユニット(CPSユニット)1, 401には、タイトル1, 211とタイトル2, 212、再生プログラム221, 222、プレイリスト231, 232、クリップ241、クリップ242が含まれ、これらの2つのクリップ241, 242に含まれるコンテンツの実データであるAVストリームデータファイル261, 262がコンテンツ管理ユニット(CPSユニット)1, 401に対応付けて設定される暗号鍵であるユニット鍵:Ku1を適用して暗号化される。

[0099] また、コンテンツ管理ユニット(CPSユニット)2, 402には、ゲームコンテンツ、WEBコンテンツなどによって構成されるアプリケーションファイル213と、再生プログラム223、プレイリスト233、クリップ243が含まれ、クリップ243に含まれるコンテンツの実データであるAVストリームデータファイル263がコンテンツ管理ユニット(CPSユニット)2, 402に対応付けて設定される暗号鍵としてのユニット鍵:Ku2を適用して暗号化される。さらに、アプリケーションファイル213についても、ユニット鍵:Ku2を適用した暗号化ファイルとしてもよい。

[0100] コンテンツ管理ユニット(CPSユニット)3, 403は、上位層の(A)アプリケーション層に含まれるアプリケーションファイル214, 215と、再生プログラム224、さらに、再生プログラム224によって情報記録媒体、あるいはネットワーク接続サーバから取得可能な様々なデータファイル、例えばJPEG, PNG, BMPなどの画像ファイル225、PCM、圧縮Audioなどの音声ファイル226、テキスト、データベースなどの各種データファイル227が含まれるユニットとして設定される。

[0101] コンテンツ管理ユニット(CPSユニット)3, 403は、コンテンツ管理ユニット(CPSユニット)3, 403に対応付けて設定される暗号鍵としてのユニット鍵:Ku3を適用して暗号化される。

[0102] 例えば、ユーザがコンテンツ管理ユニット1，401に対応するアプリケーションファイルまたはコンテンツ再生処理を実行するためには、コンテンツ管理ユニット(CPSユニット)1，401に対応付けて設定された記録シードVu1を適用した暗号処理により、ユニット鍵:Ku1を取得して、取得したユニット鍵Ku1を適用したコンテンツの復号処理シーケンスを実行することが必要であり、復号処理を実行後、アプリケーションプログラムを実行してコンテンツ再生を行なうことができる。

[0103] 例えば、コンテンツ管理ユニット3，403に対応するアプリケーションファイルまたは、再生プログラム224に対応付けられた画像ファイル225、PCM、圧縮Audioなどの音声ファイル226、テキスト、データベースなどの各種データファイル227の利用処理を行なう場合は、コンテンツ管理ユニット(CPSユニット)3，403に対応付けて設定された暗号鍵としてのユニット鍵:Ku3を取得して、復号処理を実行することが必要であり、復号処理を実行後、アプリケーションプログラムを実行または各種ファイルを実行することになる。

[0104] 上述した各種のコンテンツ管理ユニット(CPSユニット)に対応するコンテンツおよび鍵情報などの管理情報を格納するディレクトリ構成例について、図5を参照して説明する。

[0105] 図5に示すディレクトリ構成は、メインコンテンツデータ部502、サブコンテンツデータ部503と、メインコンテンツとサブコンテンツに対応するコンテンツ管理データ部501を設定した構成である。メインコンテンツデータ部502に示すBDMVディレクトリはBlu−ray Disc ROMフォーマットに従ったコンテンツ、アプリケーションを保管するディレクトリとして設定されている。

[0106] Blu−ray Disc ROMフォーマットに従ったメインコンテンツは、先に図3、図4を参照して説明したように、タイトル、オブジェクト、プレイリスト、クリップ情報、AVストリーム等の階層構成を持ち、これらを構成するデータファイルがBDMVディレクトリに設定される。

[0107] サブコンテンツデータ部503のDataディレクトリは、Blu−ray Disc ROMフォーマットに従っていないフォーマットを持つコンテンツ、アプリケーションを各グループ毎に保管するディレクトリとして設定されている。サブコンテンツデータ部503のData

Group infは、サブコンテンツの各グループ情報を格納したファイルである。

[0108] 管理データ部501には、メインコンテンツとサブコンテンツの両コンテンツに対応する管理ファイルが格納される。例えば、前述した図2に示したコンテンツ管理ユニット(CPSユニット)毎のCPSユニットIDと記録シード情報を対応付けて設定したCPSユニット管理テーブル、さらに、各ユニットに対応して設定されるコンテンツの再生制御情報、コピー制御情報が格納される。

[0109] コンテンツの再生制御情報、コピー制御情報は、各CPSユニット毎に個別の情報として設定される。例えば、

[CPSユニット1]

記録媒体に対するコピー許容回数:a回、再生許容回数:b回、遠隔再生可否:可・・

[CPSユニット2]

記録媒体に対するコピー許容回数:0回、再生許容回数:c回、遠隔再生可否:否・・

などのように、情報記録媒体に格納された各CPSユニット毎に個別のコンテンツ利用制御情報が設定されている。

[0110] [4. 後発的に生成したデータまたは取得したデータの管理構成]

上述したように、情報記録媒体に格納済みのコンテンツは、CPSユニットに区分され、各CPSユニットに対応する暗号鍵としてのCPSユニット鍵を記録シードを適用して取得することで、利用可能となる。

[0111] 情報記録媒体に格納済みのコンテンツとは異なるデータ、例えば、情報記録媒体に格納されたプログラムに従って生成されたデータ、具体的には、ゲームプログラムを実行して生成した途中経過のデータや、キャラクタデータ、あるいは、ネットワークを介してサーバなどから取得したデータ、このような、何らかのユーザの処理によって後発的に生成または取得したデータの管理処理について、以下説明する。

[0112] 図6に情報記録媒体に格納済みのコンテンツに関連するデータの生成、取得処理例を示す。

[0113] 図6には、情報記録媒体の再生処理を実行する例えばPC等の情報処理装置600

を示している。情報処理装置600は、コンテンツ再生処理を実行する例えばCPUなどのプログラム実行機能を持つ制御部601、ハードディスク等によって構成されるデータ記憶部602、情報記録媒体に対するデータ入出力を行なう記録媒体インタフェース603、プログラムの実行領域、パラメータ格納領域などに利用されるROM, RAMによって構成されるメモリ604、ネットワークを介した通信を実行する通信インタフェース605を有する。なお、図6に示す情報処理装置600の構成は、後発データの生成、取得処理について説明するための最小限の構成を示しているものであり、具体的な情報処理装置のハードウェア構成例については後段で説明する。

[0114] 情報処理装置600は、情報記録媒体100から記録媒体インタフェース603を介して情報記録媒体100に格納されたCPSユニットに区分されたコンテンツを読み取り、コンテンツの再生処理を、制御部601の制御の下に行なう。

[0115] 情報記録媒体100には、例えば、図3、図4を参照して説明したように、Blu-ray Disc ROM規格に基づいて記録されたコンテンツが格納されている。各コンテンツはCPSユニットに区分され暗号化処理が施されている。

[0116] 情報処理装置600は、CPSユニット対応の記録シードに基づいてCPSユニット鍵を生成して、コンテンツを再生する。コンテンツには例えばゲーム、あるいはAVストリーム再生プログラムなどの各種のプログラム、AVストリームデータなどが含まれる。

[0117] 情報処理装置600が、情報記録媒体100からのデータ読み取りに基づいて、後発的にデータを生成、あるいは取得する態様としては次の2つの態様がある。

[0118] 1つ目は、情報処理装置600が解析可能な情報を、情報記録媒体100から読み取り、読み取り情報に基づいて、新規データを取得または生成する場合である。例えば情報記録媒体100内に後発データの取得先に対応するURL情報が記述してあり、情報記録媒体100が、このURL情報を取得して、ブラウザーを使用して通信IF605およびネットワークを介してURLによって指定されるサーバ611などにアクセスし、URL対応の新規コンテンツなどのデータをダウンロードする処理である。コンテンツダウンロード以外にも、情報記録媒体100からの読み取り情報に基づいて、情報処理装置600内で新規データを生成する場合がある。

[0119] 2つ目は、情報記録媒体100内に記録されたアプリケーションプログラムによるもの

である。例えば、情報処理装置600において、情報記録媒体100から読み取ったプログラムを実行し、プログラムに従って、通信IF605およびネットワークを介して特定のサーバ611に接続しコンテンツをダウンロードする、あるいは、情報処理装置600において、プログラムの実行により後発的なデータが生成される場合がある。

[0120] このような様々な処理により生成または取得されたデータは、情報記録媒体100内に記録されたコンテンツの管理区分であるCPSユニットに属するデータではないが、本発明の構成においては、これら後発的なデータを特定のCPSユニットに属するデータとして管理する。

[0121] 具体的には、情報記録媒体100に格納されたCPSユニット対応のコンテンツに基づいて生成または取得した後発データについては、同一のCPSユニットに属するデータとして管理する。あるいは新規なCPSユニットを別途定義して新たなCPSユニットにより管理する。

[0122] 図7に情報記録媒体の格納コンテンツに基づいて、外部サーバから後発データを取得する処理シーケンスを示す。ステップS101において、情報処理装置は、情報記録媒体からCPSユニットによって管理されたコンテンツを読み出す。例えばCPSユニットAに属するコンテンツを読み出したものとする。

[0123] 情報処理装置は、ダウンロードデータの指定情報、例えばURLなどを情報記録媒体から読み出すとともに、読み出しコンテンツに対応するCPSユニットの識別子としてのCPSユニットIDを取得し、ステップS102において、これらのデータ、すなわちCPSユニットIDと、ダウンロードデータ指定情報をサーバに送信する。

[0124] サーバは、予め定められた認証シーケンスによって、正当な情報記録媒体から取得したCPSユニットIDであるかなどの認証処理を実行し、データ要求の正当性を検証し、正当性が確認された場合に、ステップS103において、要求されたダウンロードデータを情報処理装置に送信する。例えばこのダウンロードデータは、AVストリームの吹き替え音声データであったり、字幕データであったり、あるいは特定のコンテンツの再生プログラムなどである。

[0125] 情報処理装置は、ステップS104において、サーバから取得したダウンロードデータを情報記録媒体、あるいは、情報処理装置内のハードディスクなどの記憶部に格納

する。いずれの場合もCPSユニットIDによって特定される同一のCPSユニットAに属するデータとして格納、管理され、CPSユニットAに対して設定される記録シードVu(a)を適用して生成されるCPSユニット鍵Ku(a)を適用した暗号処理によってか暗号化されて格納される。

[0126] 図7を参照して説明したシーケンスでは、情報処理装置がサーバに対してダウンロードデータを要求する際、CPSユニットIDとダウンロードデータ指定情報を送信する設定としてあるが、これは、CPSユニットIDの送信を行なうことで、以下のような管理が可能となるからである。

(1)サーバにおいてCPSユニットごとにダウンロードデータの管理が可能となる。

(2)CPSユニットごとに、ダウンロードの可否、課金処理などを管理している場合、いったんダウンロード可能となったCPSユニットに関しては次回よりCPSユニットIDを送信するだけでダウンロードを開始することができる。

(3)情報記録媒体上でCPSユニットごとに定義された鍵(ユニット鍵)を用いてダウンロードデータの暗号化を行う場合、サーバで暗号化処理を行うためにはCPSユニットIDが必要となる。サーバではユニットIDに対応したCPSユニット鍵を保持し、保持したCPSユニット鍵を適用して暗号化したデータを送信することでセキュアなデータ送信が可能となる。

[0127] なお、ダウンロードデータ指定情報としては、URLなどの情報以外に、例えば、Blu-ray Disc ROM規格等で定められた値であるスタジオID、パッケージID、タイトルID、ムービーオブジェクトのID、プレイリストのID、再生区間情報(開始点、終了点のタイムスタンプ)、なども適用可能であり、また、Blu-ray Disc ROM規格等で定められていない値をダウンロードデータ指定情報として用いてもよい。例えば、ユーザID、課金状況などのユーザ付属情報、日時情報、コンテンツ再生において情報処理装置側で生成される管理データ、例えば再生回数、再生済み範囲、ゲームの得点、マルチストーリーの再生パス情報など、サーバ側でダウンロードデータを特定可能な情報であれば、様々なデータがダウンロードデータ指定情報として適用できる。

[0128] 次に、情報処理装置が生成または取得するデータの具体例について、図8、図9を参照して説明する。

[0129] 図8には、Blu-ray Disc ROM規格フォーマットに従ったデータの一部を後発データとして生成または取得する例を示している。先に、図3、図4を参照して説明したように、Blu-ray Disc ROM規格フォーマットに従って情報記録媒体に格納されたコンテンツは階層構成を持ち、各階層のデータ、プログラムが関連付けられて例えばAVストリームのコンテンツ再生処理が可能となる。

[0130] 図8に示す情報記録媒体621には、Blu-ray Disc ROM規格フォーマットに従ったコンテンツとして、3つのタイトル[タイトル1]、[タイトル2]、[タイトル3]に対応付けられたCPSユニット1, 2, 3が設定されている。

[0131] この3つのCPSユニット中、2つのタイトル[タイトル1]、[タイトル2]に対応付けられたCPSユニット1, CPSユニット2には、各タイトルに対応する再生プログラムとしてのムービーオブジェクト1, 2が格納され、ユーザは、情報処理装置に情報記録媒体をセットし、[タイトル1]または[タイトル2]を指定することで、再生プログラムとしてのムービーオブジェクト1, 2のいずれかを実行させて、プレイリストによって指定される区間のクリップファイル、すなわちAVストリームデータを再生することができる。ただし、それぞれのCPSユニットに対応する記録シードを管理データから取り出してCPSユニット鍵を生成してAVストリームなどの暗号化データを復号することが必要である。

[0132] しかし、CPSユニット3には、タイトル3に対応する再生プログラムとしてのムービーオブジェクト3が格納されておらず、CPSユニット内に含まれるクリップファイル、すなわちAVストリームデータを再生することができない。この場合、情報処理装置は、タイトル3に対応する再生プログラムとしてのムービーオブジェクト3の生成または取得処理を実行し後発データ622としてムービーオブジェクト3を生成または取得する。生成または取得したムービーオブジェクト3は、CPSユニット3の構成データとして管理される。

[0133] 図9は、後発的に情報処理装置が生成または取得するデータのその他の具体例について示した図である。

[0134] 情報処理装置600は、複数のCPSユニットによって管理されたコンテンツを格納した情報記録媒体100を再生する。

[0135] 例えば、CPSユニットA640はゲームプログラムを含むコンテンツ管理ユニットであり

、情報処理装置600がゲームプログラムを実行することにより、ゲームの途中終了情報、ゲーム得点情報などの後発データ641，642が生成される。これらのデータは、情報処理装置600において、CPSユニットA640の構成データとして設定する処理が実行されて、情報記録媒体100または情報処理装置600内のハードディスクなどの記憶部に格納される。

[0136] また、CPSユニットB650は映画などの動画等のAVストリームコンテンツを含むコンテンツ管理ユニットであり、情報処理装置600は、AVストリームコンテンツに対応する字幕データからなる後発データ651をサーバ611から取得して、再生を行なう。取得した字幕データ651は、情報処理装置600において、CPSユニットB650の構成データとして設定する処理が実行されて、情報記録媒体100または情報処理装置600内のハードディスクなどの記憶部に格納される。

[0137] なお、いずれの処理の場合においても、後発的に生成したデータまたは取得したデータについて新たなCPSユニットを設定し、設定した新規CPSユニットの構成データとして情報記録媒体100または情報処理装置600内のハードディスクなどの記憶部に格納する構成としてもよい。これらのユニットとしては、先に図2を参照して説明した新規データに対応するCPSユニットが対応付けられて設定される。それぞれのCPSユニットに対応する記録シードVuは予め情報記録媒体に格納されており、その記録シードを適用して、予め定められた暗号処理シーケンスを実行してCPSユニット鍵を生成し、生成したCPSユニット鍵を適用して、生成データまたは取得データの暗号化を実行して情報記録媒体100または情報処理装置600内のハードディスクなどの記憶部に格納する。

[0138] なお、新たに設定するCPSユニットに対応する記録シードVuについては、外部のサーバから取得する設定としてもよい。ただし、記録シードVuを提供するサーバと情報処理装置間において所定の認証処理を実行し、不正な記録シード取得を防止した構成とすることが望ましい。ここで、取得する記録シードVuは、図2で示す管理テーブルの単位での取得も含む。

[0139] 後発的に生成したデータまたは取得したデータの暗号化および管理態様について図10を参照して説明する。

[0140] 図10には、情報記録媒体に格納されたコンテンツの再生処理に対応して生成または取得するデータを情報記録媒体内部または外部に記録する場合のデータ暗号化方法の例を示している。

[0141] 図10において、左側のデータ領域は、情報記録媒体に格納済みのデータ、すなわちROM領域データ660であり、右側のデータ領域は、新規生成または取得データとしての後発データ670である。新規生成または取得データは、情報記録媒体のデータ書き込み可能な領域またはハードディスク、あるいは携帯メモリなど外部の記憶手段に格納される。図10には、新規生成または取得データに対するCPSユニット設定例として2つの例を示している。

[0142] (設定例1)

図10に示すCPSユニット3, 681に示すように、後発データ671を、情報記録媒体に設定済みのCPSユニットに一体化する処理例である。

[0143] CPSユニット3, 681は、情報記録媒体に格納済みのデータ、すなわち、データ領域660において設定済みのCPSユニット3であり、このCPSユニット3, 681に、新規生成または取得した後発データ671を含めて、1つのユニットとする構成である。この場合、後発データ671、または後発データ671に含まれるデータは、CPSユニット3に対応して設定されている記録シードVu3を適用して生成されるユニット鍵Ku3を用いて暗号化されて情報記録媒体またはハードディスクなどの記憶部に格納される。

[0144] この構成例では、情報記録媒体のROM領域において定義済みのCPSユニットに対応するユニット鍵と同じ鍵を使用して生成データの暗号化を行う構成であり、再生処理においては、情報記録媒体のROM領域において定義済みのCPSユニットに含まれていたデータと同様の鍵を適用して後発データ671の復号処理を実行することが可能であり、鍵の切り替え処理が不要となりシームレスな再生が可能となる。

[0145] (設定例2)

図10に示すCPSユニット4, 682に示すように、後発データ672を、情報記録媒体に設定済みのCPSユニットとは異なる新規のCPSユニットを設定して管理する処理例である。

[0146] このように後発データ672用に別途CPSユニット4, 682を定義し、それに対応した

ユニット鍵を用いて後発データ672に含まれるデータの暗号化を行う。CPSユニット4，682は、情報記録媒体に記録されているデータとは独立な管理がなされる。この場合、後発データ672用にCPSユニットを割り当てるための情報、およびユニット鍵を生成するための情報を別途、管理データとして設定して記録する必要がある。

[0147] 図11を参照して、新規生成または取得した後発データに対応する管理データとしての再生／コピー制御情報の設定例について説明する。

[0148] 図11には、予め情報記録媒体100に格納されたCPS管理ユニット構成に対応するディレクトリAと、新たに生成または取得した後発データに対応するディレクトリBとを示している。図11に示す例は、いずれもBlu-ray Disc ROM規格フォーマットに従ったコンテンツとして[BDMV]ディレクトリに各データが設定され、[CPS]ディレクトリに各種の管理データが格納される。

[0149] 再生／コピー制御情報を記録する方法としては、以下の2つの設定例のいずれかを適用する。

（設定例1）

既存の再生／コピー制御情報を後発データの再生／コピー制御情報として適用する。

これは、図11に示すように情報記録媒体100に予め格納されたCPSユニット001のデータ[01001.m2ts]715に対応する再生／コピー制御情報[CPSUnit001.cci]713をそのまま、新たに生成または取得した後発データ[01003.m2ts]712に対応する再生／コピー制御情報として適用する。この場合、後発データ[01003.m2ts]712に対応する再生／コピー制御情報を新たに生成することは不要であり、CPSユニット001の再生／コピー制御情報[CPSUnit001.cci]713が、既存データ[01001.m2ts]715と、後発データ[01003.m2ts]712の双方に適用される再生／コピー制御情報として設定される。

[0150] （設定例2）

後発データの再生／コピー制御情報を新たに生成する。

これは、図11に示すように後発データ[01002.m2ts]711に対応する再生／コピー制御情報として、新たな再生／コピー制御情報[CPSUnit002.cci]714を生成

して、管理データとする例である。

[0151] (設定例1)のケースは、例えば情報記録媒体100のROM領域に記録されていない言語の字幕データをダウンロードして取得し、ROM領域に記録されている映像・音声データと合わせて再生する場合などに適した方法である。この場合、ROM領域に記録されたデータ、ダウンロードしたデータの両方が1つのCPSユニットに属すると考えて処理を行うことが自然である。

[0152] また、(設定例2)のケースは、情報記録媒体100から読み出したアプリケーションプログラムを実行して生成したデータを複数のユーザ間で共有／コピーが可能となるようにしたい場合などに適している。実行アプリケーションやAVストリームなどのROM領域に記録されたデータはコピー不可であるが、実行アプリケーションによって生成されるデータ(ゲームの得点情報、地図情報など他のユーザへの送信や、携帯機器などへの持ち出しニーズがある情報)はROM領域と異なる再生／コピー制御が可能となる。

[0153] 図12は、暗号鍵、すなわち各CPSユニットに対応するユニット鍵の生成情報としての記録シードの設定例を示した図である。

[0154] 図11と同様、予め情報記録媒体100に格納されたCPS管理ユニット構成に対応するディレクトリAと、新たに生成または取得した後発データに対応するディレクトリBとを示している。図12に示す例は、いずれもBlu-ray Disc ROM規格フォーマットに従ったコンテンツとして[BDMV]ディレクトリに各データが設定され、[CPS]ディレクトリに各種の管理データが格納される。

[0155] 記録シードは、先に図2を参照して説明したようにCPSユニット管理テーブルにおいて、各CPSユニット識別子(CPSユニットID)に対応付けて管理される。図12に示す暗号鍵情報[Unit Key Gen Value. inf]721が、情報記録媒体100に格納されたCPSユニット管理テーブルである。

[0156] 後発データに対応して設定されるCPSユニット対応の記録シードの設定方法としては、以下の2つの設定例のいずれかを適用する。

[0157] (設定例1)

後発データの暗号鍵生成情報としての記録シードとして、CPSユニット管理テーブ

ルに予め設定済みの新規データ用の記録シードを使用する。

これは、先に図2を参照して説明したCPSユニット管理テーブル中の新規データ用フィールド121(図2参照)に設定済みの記録シードを後発データの暗号鍵生成情報としての記録シードとして使用する構成である。図12において、後発データ[01003.m2ts]724に対応させて、情報記録媒体100に格納されている管理テーブルデータである暗号鍵情報[Unit Key Gen Value.inf]721の新規データ用フィールド121(図2参照)に設定済みの記録シードを対応付ける。この設定例では、新たなCPSユニットを定義して、新規データ用フィールド121(図2参照)に設定済みの記録シードを適用することが可能である。

[0158] (設定例2)

後発データの暗号鍵生成情報としての記録シードとして、新たに生成または取得した記録シードを使用する。図12において、後発データ[01002.m2ts]723に対応させて、新たな管理テーブルデータとしての暗号鍵情報[Unit Key Gen Value.inf]722を設定し、新規エントリとして新規設定したCPSユニット識別子と生成または取得した記録シードとを対応付けて格納する。なお、記録シードの生成が許容される場合、情報処理装置は、情報処理装置内のデータ処理部において、例えば乱数を生成して新たな記録シードを生成する。この設定例においては、新たなデータについて、無制限にCPSユニットの設定、記録シードの生成が可能となる。

[0159] なお、情報処理装置において、新たなCPSユニットを設定した場合は、その新規設定CPSユニットに対応する管理データ、すなわち、再生/コピー制御情報を対応付けることが必要となるが、これは、前述した図11の2つの手法のいずれか、すなわち既存の再生/コピー制御情報を対応付けるか、あるいは新規の再生/コピー制御情報を設定して対応付けるかのいずれかの方法が適用される。

[0160] [5.ナビゲーションファイルの暗号化および改竄防止構成]

図11、図12を参照して説明した例では、後発的なデータ中、AVストリームデータファイルのみの暗号化構成を説明した。例えば図11に示す後発データ[01002.m2ts]711、後発データ[01003.m2ts]712等のAVストリームデータを暗号化して情報記録媒体のデータ書き込み可能な領域またはハードディスク、あるいは携帯メモ

リなど外部の記憶手段に格納する構成例である。

[0161] しかし、後発的データには、AVストリームデータのみならず、タイトルインデックス、ムービーオブジェクト、プレイリストファイル、クリップ情報ファイルなどのファイルも含まれる。これらのファイルについても正規の再生アプリケーションソフトからのみアクセス可能とし、例えばPC上で動作する他の様々なアプリケーションからのアクセスを排除する構成とすることが好ましい。またAVストリームデータを含むファイルについて改竄を防止し、改竄検証を可能とした構成とすることが好ましい。なお、AVストリーム以外のファイルであるタイトルインデックス、ムービーオブジェクト、プレイリストファイル、クリップ情報ファイルを総称してナビケーションファイルと呼ぶ。図13、図14を参照してこれらナビケーションファイルについての暗号化格納構成、および電子署名データの付与による改竄防止、検証構成について説明する。

[0162] 図13は、AVストリームデータファイルに加え、AVストリーム以外のナビゲーションファイルであるタイトルインデックス、ムービーオブジェクト、プレイリストファイル、クリップ情報ファイルの各々について、各ファイル毎に個別に暗号化して格納する構成例を説明する図である。

[0163] 図13に示す記憶手段750は、後発データを格納する情報記録媒体のデータ書き込み可能な領域またはハードディスク、あるいは携帯メモリなど外部の記憶手段に相当する。記憶手段750に記憶される後発データとしては、図に示すAVストリームデータファイル755に加え、AVストリーム以外のナビゲーションファイルであるタイトルインデックスファイル751、ムービーオブジェクトファイル752、プレイリストファイル753、クリップ情報ファイル754が含まれる。これらのナビゲーションファイル、AVストリームデータファイルのすべてをファイル単位で暗号化して格納する。プレイリストファイル753、クリップ情報ファイル754は、AVストリームデータファイル755と同様、CPSユニット毎に個別のファイルとして設定され、暗号化は、各ファイル単位で実行する構成となっている。

[0164] この暗号化処理に適用する暗号鍵は、正当なライセンスを受けた再生アプリケーションソフトのみが生成または取得可能とした構成が好ましい。例えば、正当なライセンスを受けた再生アプリケーションソフトのみが取得可能な情報を暗号鍵とするか、ある

いは、このような限定された情報に基づいて暗号鍵を生成する。その1つの具体例が各CPSユニット対応のユニット鍵を暗号鍵として適用する構成である。図13に示すAVストリームデータファイル755、および、AVストリーム以外のナビゲーションファイルであるタイトルインデックスファイル751、ムービーオブジェクトファイル752、プレイリストファイル753、クリップ情報ファイル754のそれぞれを各ファイルが属するCPSユニットに対応付けられたユニット鍵を適用して暗号化を実行して格納する。再生処理の実行時には、各ファイルに対応するCPSユニットのユニット鍵を取得して、取得ユニット鍵を適用した復号処理を実行する。

[0165] さらに、CPSユニットに対応するユニット鍵を適用することなく、その他の情報を鍵生成情報として用いる構成としてもよい。ただし、CPSユニットのデータファイルの再生を許容された正当な再生アプリケーション以外のその他のアプリケーションによって暗号鍵の生成を可能とした構成は好ましくない。従って、正当なライセンスを受けた再生アプリケーションソフトによってのみ取得可能な情報を鍵生成情報として設定する。正当なライセンスを受けた再生アプリケーションソフトによってのみ取得可能な情報としては、例えば、デバイスIDがある。

[0166] デバイスIDは、正当なライセンスを受けた再生アプリケーションソフトに対応して設定されるIDであり、例えば再生アプリケーションを正当にインストールしたデバイスとしてのハードウェアに設定された識別情報などに基づいて生成される。このデバイスIDは、正当なインストール処理のなされた正当な再生アプリケーションソフトウェアに記録されたプログラムによってのみ取得可能とする。

[0167] 従って、デバイスIDは、正当なライセンスを受けた再生アプリケーションソフトによってのみ取得、生成可能なデータであり、例えば様々なアプリケーションソフトウェアがインストールされたPCにおいて、他のアプリケーションによる取得は排除される。後発データを生成または取得した場合には、正当な再生アプリケーションが、デバイスIDを取得して暗号鍵生成処理を実行して暗号鍵を生成し、生成した暗号鍵を適用してAVストリームデータファイル755、および、AVストリーム以外のナビゲーションファイルであるタイトルインデックスファイル751、ムービーオブジェクトファイル752、プレイリストファイル753、クリップ情報ファイル754のそれぞれを暗号化して記憶手段750

に格納する。暗号鍵生成アルゴリズムとしては例えばAES暗号鍵生成アルゴリズムなどが適用可能である。具体的には、例えば、データ量が多いAVストリームデータファイル755については6KB単位のブロック暗号化、その他のナビゲーションファイルについては2KB単位のブロック暗号化とするなどの構成とする。

[0168] 暗号化ファイルを復号する場合には、正当な再生アプリケーションソフトウェアによって、デバイスIDを取得して、暗号鍵の生成を実行し、生成した暗号鍵によって暗号化ファイルの復号処理を実行する。

[0169] なお、上述のデバイスIDのみならず、その他の情報、例えばCPSユニット管理コンテンツを格納した情報記録媒体の格納コンテンツの編集スタジオの識別子としてのスタジオID、情報記録媒体の製造単位として設定されるパッケージ識別子としてのパッケージIDやボリュームIDなどをデバイスIDとを組み合わせて暗号鍵の生成を行なう構成としてもよい。

[0170] なお、後発ファイルを設定したディレクトリに様々なスタジオ(コンテンツ提供エンティテイ)に関連するファイルが設定される場合には、各ファイルに対応するスタジオIDを適用する構成とするこが好ましい。パッケージID、ボリュームIDを適用する場合も同様である。これらの様々なIDを暗号鍵生成情報として適用する場合、ディレクトリに設定した後発ファイルが、どのスタジオID、パッケージID、ボリュームIDに基づいて生成された暗号鍵が適用されているかを判別可能な構成とすることが必要となる。

[0171] 後発データファイルの暗号鍵の生成情報として適用したスタジオIDなどをそのままディレクトリ名や、ファイル名に使用する構成も可能であるが、このような設定とした場合には、コンテンツの再生処理時にスタジオ名等が判明する可能性があり、判明したデータに基づいて暗号鍵生成情報を類推されてしまう可能性がある。これを避けるため、ディレクトリ名やファイル名は別途割り当てる番号や乱数を用いて決定し、スタジオIDなど暗号鍵生成情報とファイルとの対応は別のテーブルとして保存する構成とすることが好ましい。

[0172] さらに、これらAVストリームデータファイル755、および、AVストリーム以外のナビゲーションファイルとしてのタイトルインデックスファイル751、ムービーオブジェクトファイル752、プレイリストファイル753、クリップ情報ファイル754各々について、デー

タ改竄を防止し、また改竄の検証を可能とするため、後発データの格納時に、後発データの全体、または特定サイズ(例えば64KB)毎に分割して、ハッシュ値を計算し、生成ハッシュ値を上述の暗号鍵によって暗号化して格納する構成とする。このハッシュ値算出処理、暗号化処理も正当なライセンスを受けた再生アプリケーションによって実行される。

[0173] ハッシュ値の暗号化には、前述のファイル暗号化の暗号鍵と同様、CPSユニットに対応して設定されるユニット鍵、あるいはデバイスID、あるいはデバイスIDとスタジオID、パッケージID、ボリュームIDの少なくともいずれかとの組み合わせに基づいて生成される暗号鍵を適用する。

[0174] データ再生時には、暗号化されたハッシュ値を復号して得られたハッシュ値と、再生対象ファイルに基づいて再計算されたハッシュ値との照合を実行し、両ハッシュ値が一致した場合にファイルの改竄がないと判定する。ファイルの改竄がないことの確認を条件としてファイルの利用、後発ファイル、後発データの利用が許容される。なお、これらの処理を実行するのは正当な再生アプリケーションソフトである。

[0175] 次に、図14を参照して、後発データ中、AVストリームデータファイルのみを暗号化し、その他のナビゲーションファイルであるタイトルインデックスファイル、ムービーオブジェクトファイル、プレイリストファイル、クリップ情報ファイルについては、暗号化を行なわず、データ改竄防止、検証用の署名を設定したファイルとして格納する構成例について説明する。

[0176] 図14に示す記憶手段770は、後発データを格納する情報記録媒体のデータ書き込み可能な領域またはハードディスク、あるいは携帯メモリなど外部の記憶手段に相当する。記憶手段770に記憶される後発データは、図に示すAVストリームデータファイル775に加え、AVストリーム以外のナビゲーションファイルであるタイトルインデックスファイル771、ムービーオブジェクトファイル772、プレイリストファイル773、クリップ情報ファイル774が含まれる。

[0177] 図14に示す例では、AVストリームデータファイル775のみをファイル単位で暗号化する。暗号鍵は、図13を参照して説明したと同様、CPSユニット対応のユニット鍵、あるいはデバイスID、あるいはデバイスIDとスタジオID、パッケージID、ボリュームI

Dの少なくともいずれかとの組み合わせに基づいて生成される暗号鍵を適用する。

[0178] AVストリームデータファイル775以外のナビゲーションファイルであるタイトルインデックスファイル771、ムービーオブジェクトファイル772、プレイリストファイル773、クリップ情報ファイル774については暗号化を行なわない。ただし、これらのナビケーションファイルについては、データ改竄防止及びデータ改竄の検証を可能とするため電子署名を付加して格納する。

[0179] これらの後発データを、例えばスタジオの管理するサーバなど、外部サーバからダウンロードして取得する場合は、予めサーバにおいて署名が施されたデータとして取得する。なおこの場合、署名検証用の鍵についても併せて取得するか、あるいは別途取得する構成とする。あるいは、ダウンロードデータあるいは自ら生成した後発データに対して、情報処理装置のデータ処理部の実行するアプリケーションにおいて自ら電子署名を生成し記憶手段に格納する構成としてもよい。

[0180] 署名生成鍵、署名検証鍵は、例えば前述の暗号鍵と同様、CPSユニット対応のユニット鍵、あるいはデバイスID、あるいはデバイスIDとスタジオID、パッケージID、ボリュームIDの少なくともいずれかとの組み合わせに基づいて生成される鍵を適用する構成が可能である。あるいは公開鍵暗号方式に従った秘密鍵と公開鍵とのペアをそれぞれ署名生成鍵、検証鍵として適用する構成としてもよい。

[0181] 署名の付加されたファイルを利用する場合には、署名の付加されたファイルの署名検証処理を実行し、ファイルデータの改竄の有無を判定する。ファイルの改竄がないことの確認を条件としてファイルの利用が許容される。なお、これらの処理を実行するのは正当な再生アプリケーションソフトである。

[0182] このように、本発明の情報処理装置は、データ処理部において正当な再生アプリケーションソフトを実行し、後発データを含むAVストリームデータファイル、およびAVストリームデータの再生処理に適用する制御情報またはプログラムを含むナビケーションファイルの暗号化処理を実行して記憶手段に記録する。あるいは、ハッシュ値または電子署名データなどの改竄検証用データを対応付けたファイルとして記憶手段に格納する。これらのファイルの利用に際しては、改竄検証を実行し、データ改竄のないことを確認したことを条件としてファイルの利用を行なう。

[0183] 本構成により、例えば、PCなど様々なアプリケーションソフトが利用可能な装置において、ライセンスされたアプリケーション以外のアプリケーションを適用してCPSユニット対応のAVストリームデータファイルやナビケーションファイルを利用したり、データ変更を行なうなどの不正なコンテンツ利用、改竄処理を防止することが可能となり、ナビケーションファイルを含むCPSユニット対応データの不正利用の排除が可能となる。

[0184] [6. 情報処理装置が生成または取得した後発データの格納処理]

次に、図15に示すフローチャートを参照して、情報処理装置が生成または取得した後発データの格納処理シーケンスについて説明する。

[0185] 情報処理装置が生成または取得した後発データの保存先は、CPSユニット管理データを格納している情報記録媒体に設定されたデータ書き込み可能領域、あるいは、外部の記憶領域のいずれかである。

[0186] 情報記録媒体外部の記憶領域とは、たとえば情報処理装置に内臓されたハードディスクや、メモリーカードのような持ち運び可能なメディアなどである。情報記録媒体内部の記憶領域とは、例えば情報記録媒体がBlu-ray Discであり、再生専用領域(ROM)と書き込み専用領域の2つの領域を有するパーシャルROM(Partial ROM)ディスクである場合のように、データ書き込み可能領域を有する情報記録媒体を適用している場合の処理である。

[0187] パーシャルROMディスクのようにデータ書き込み可能領域を有する情報記録媒体を適用している場合であれば、保存先を情報記録媒体か情報記録媒体以外かの2つから選択することができるが、データ書き込み可能領域を有する情報記録媒体を適用していない場合は、必然的に情報記録媒体以外の記憶領域に生成データが保存される。

[0188] 図15に示すフローに従って、情報処理装置が生成または取得した後発データの格納処理シーケンスについて説明する。

[0189] ステップS201において、情報処理装置が情報記録媒体から読み取ったデータまたはプログラムに従って、後発データを生成または取得する。ステップS202において、データの記録を実行するか否かを判定する。この判定処理は例えばデータ入力

手段からのユーザ入力などによって決定される。あるいは予め設定された情報に基づく自動決定処理として実行してもよい。

[0190] データの記録を実行しない場合は、記録処理を行なうことなく処理を終了する。データ記録を行なう場合は、ステップS203に進み、情報処理装置に装着している情報記録媒体が、パーシャルROMディスクのようにデータ書き込み可能領域を有する情報記録媒体であるか否かを判定する。

[0191] データ書き込み可能領域を有する情報記録媒体でない場合は、ステップS205に進み、生成または取得したデータを、そのデータに対応付けられたCPSユニットの構成データとして情報記録媒体以外の記憶手段にデータを格納する。なお、このデータ格納処理においては、格納データに対応するCPSユニット管理情報として、再生／コピー制御情報と、CPSユニット管理テーブルにおける記録シードがそれぞれ対応付けられることとなる。この対応付けの構成については後述する。

[0192] ステップS203において、情報処理装置に装着している情報記録媒体が、パーシャルROMディスクのようにデータ書き込み可能領域を有する情報記録媒体であると判定された場合は、ステップS204に進み、データ書き込みを情報記録媒体に対して行なうか否かを判定するこれは例えばユーザ入力情報に基づく判定処理として実行される。あるいは予め設定された情報に基づく自動判定処理として実行してもよい。

[0193] データ書き込みを情報記録媒体に対して行なわない場合は、ステップS205に進み、生成または取得したデータに対応付けられたCPSユニットの対応データとして情報記録媒体以外の記憶手段にデータを格納する。

[0194] データ書き込みを情報記録媒体に対して行なう場合は、ステップS206に進み、情報記録媒体のデータ書き込み可能領域に対して、生成または取得したデータをCPSユニットの対応データとして情報記録媒体に格納する。なお、このデータ格納処理においては、格納データに対応するCPSユニット管理情報として、再生／コピー制御情報と、CPSユニット管理テーブルにおける記録シードがそれぞれ対応付けられることとなる。

[0195] [7. 情報記録媒体のCPSユニット構成データと情報記録媒体外部に格納したCPSユニット構成データの関連づけ構成]

上述したように、CPSユニットによって管理されたコンテンツを格納した情報記録媒体にオリジナルデータとして格納されていない後発データは情報記録媒体またはハードディスクなどに格納される。この新規データを情報記録媒体のCPS管理データの管理対象データとして取り扱うためには、情報記録媒体またはハードディスクなどに格納される新規データを情報記録媒体のCPS管理データの管理対象データであることを識別可能とすることが必要となる。以下、この識別の構成について説明する。

[0196] 図16は、後発データをオリジナルのCPSユニットを持つ情報記録媒体以外の記憶手段、例えば情報処理装置のハードディスクなどの記憶手段に格納する構成における後発データとCPSユニットとの関連付け構成を示す図である。

[0197] オリジナルのCPSユニットを持つ情報記録媒体以外の記憶手段に後発データを記録する場合、図16に示すように、それぞれがCPSユニットを持つ異なる情報記録媒体801，802に対応する後発データを1つのハードディスクなどの記憶手段803に格納することとなる。

[0198] この場合、記憶手段803に格納する様々な後発データが、それぞれどの情報記録媒体801，802に対応する後発データであるかを区別することが必要となる。

[0199] 情報記録媒体801，802には、先に図1を参照して説明したように、情報記録媒体100の格納コンテンツの編集スタジオの識別子としてのスタジオID、情報記録媒体100の製造単位としてのパッケージ識別子としてのパッケージIDが格納されている。

[0200] 図16に示すように、記憶手段803に格納する様々な後発データ804，805，806に対しては、スタジオID、パッケージID、さらにCPSユニットIDが識別データとして付与され、図に示すようにスタジオID、パッケージID、CPSユニットIDの順にディレクトリ階層構造を設定し、このディレクトリ階層構造に基づいてデータ格納、管理を行なう。

[0201] CPSユニットIDごとに割り当てられたディレクトリの内部には、任意の形式で生成データの保存が可能である。例えばJava等の実行アプリケーションが生成するデータであれば、そのデータは再生時にJava等の実行アプリケーションで解釈できる形式であれば良く、特定の形式に縛られるものではない。

[0202] このようにディレクトリ階層が規定される場合、オリジナルのCPSユニットを持つ情報

記録媒体以外の記憶手段に記録されたデータをJava等の実行プログラムから呼び出す場合の参照処理は、たとえば図17に示すように名前空間、ディレクトリ、ファイル名に基づいて呼び出す処理として実行可能である。すなわち、オリジナルのCPSユニットを持つ情報記録媒体のデータ書き込み領域を[Partial−ROM:／／]、ハードディスクを[Local−HDD:／／]のように名前空間を定義し、それぞれの新規データの格納ファイルを名前空間、ディレクトリ、ファイル名によって特定しファイルデータの読み込み、更新、再書き込みなどの処理が可能である。

[0203] 次に、図18を参照して、後発データをオリジナルのCPSユニットを持つ情報記録媒体のデータ書き込み可能領域に書き込む場合の後発データとCPSユニットとの関連付け構成について説明する。

[0204] 後発データをオリジナルのCPSユニットを持つ情報記録媒体のデータ書き込み可能領域に記録する場合、図16を参照して説明した複数のパッケージにわたる生成データの管理が必要ない。従ってスタジオID、パッケージIDを用いたディレクトリ管理は必要なく、図18に示すように、後発データ811，812に対しては、CPSユニットIDによって識別可能なデータとして管理する構成となる。

[0205] [8. プログラム実行条件を限定した処理構成]

次に、CPSユニットによって管理されたコンテンツを格納した情報記録媒体から読み出し可能なプログラム、例えばJavaなどの様々なアプリケーションプログラムの実行条件として、オリジナルのCPSユニットを持つ情報記録媒体であること、あるいは特定の種類の情報記録媒体であることを規定し、不正なコンテンツの利用、コンテンツのコピーを防止した構成について説明する。

[0206] 図19を参照して、オリジナルのCPSユニットを持つ情報記録媒体であることの確認を条件としたプログラム実行における処理シーケンスについて説明する。この処理は、CPSユニットによって管理されたコンテンツを格納した情報記録媒体を装着した情報処理装置において実行される処理である。

[0207] ステップS301において、CPSユニットによって管理されたコンテンツを格納した情報記録媒体を装着した情報処理装置は、情報記録媒体から読み出したプログラムを起動し、ステップS302において、プログラム実行条件確認処理として、ディスク種別

判別実行する。これは、例えば情報記録媒体の物理領域に記録されているディスク種別識別情報106(図1参照)に基づいて実行される。

[0208] ステップS303において、ディスク種別がパーシャルROMか否かを判定する。ディスク種別がパーシャルROMでない場合、ステップS306に進みプログラムの実行を中止し、処理を終了する。

[0209] ディスク種別がパーシャルROMである場合、ステップS304に進み、プログラムを実行する。ステップS305においてプログラムの終了を確認した後、処理を終了する。

[0210] 図20は、具体的な情報記録媒体の種別に対応したプログラムの実行可否設定例について説明する図である。

[0211] 情報処理装置は、装着した情報記録媒体820の物理領域から情報記録媒体のディスク種別識別情報を取得する。この種別情報には、例えば、パーシャルROMディスクである、あるいはデータ書き込み可能なRWディスク、あるいはRディスクなど、ディスクの種別を示す情報が含まれている。

[0212] 情報処理装置は、情報記録媒体820から読み取ったプログラム(例えばJava)の実行開始に際し、情報記録媒体820の種別を判定し、種別がパーシャルROMである場合に限りプログラムの実行を許容し、その他のRWディスク、あるいはRディスクなどの場合には、プログラムの実行を中止する。

[0213] この処理によって、図に示すように、パーシャルROM821が情報処理装置に装着されている場合には、パーシャルROM821から読み取られたプログラムが実行されるが、その他のRWディスク822、あるいはRディスク823の場合には、同一のプログラムが書き込まれていた場合であっても、その読み出しプログラムの実行は許容されないことになる。

[0214] 従って、オリジナルのCPSユニットを持つ情報記録媒体がパーシャルROM821であった場合、そのデータコピーを実行して、RWディスク822、あるいはRディスク823を生成しても、プログラムの実行は許容されず、コピーコンテンツの利用を防止することができる。

[0215] なお、上述の処理例は、プログラムの実行可否を情報記録媒体の種別に基づいて決定する例であるが、さらに、後発データの書き込み先を限定する構成としてもよい。

また、上述の例においては、パーシャルROMディスクを適用した場合の処理として説明しているが、ROMディスクを適用した場合においても同様の処理が可能である。

[0216] 情報記録媒体がパーシャルROMである場合、後発データをパーシャルROMのデータ書き込み可能領域に書き込むことが可能であるが、パーシャルROMから読み出したプログラムを実行する場合、そのプログラムの実行に基づいて生成したデータあるいは取得したデータなどの後発データの書き込み先をプログラムによって規定する。すなわち、パーシャルROMから読み出したプログラムの実行に基づいて生成または取得したデータの書き込み先を同一のパーシャルROMのデータ書き込み領域にのみ限定する。これは、プログラムに書き込み先条件を設定することで実現される。このような構成とすることで、ユーザが後発的に生成または取得したデータについての利用制限も可能となる。

[0217] [9. 情報処理装置の構成例]

次に、図21を参照して、上述のCPSユニットによって管理されたコンテンツを格納した情報記録媒体の再生、記録処理を行う情報処理装置の構成例について説明する。

[0218] 図21に示す情報処理装置900は、情報記録媒体910の駆動を行ない、データ記録再生信号の入手力を行なうドライブ909、各種プログラムに従ったデータ処理を実行する制御手段としてのCPU907、プログラム、パラメータ等の記憶領域としてのROM906、メモリ908、デジタル信号を入出力する入出力I／F902、アナログ信号を入出力し、A／D，D／Aコンバータ904を持つ入出力I／F903、MPEGデータのエンコード、デコード処理を実行するMPEGコーデック921、TS(Transport Stream)・PS(Program Stream)処理を実行するTS・PS処理手段922、各種の暗号処理を実行する暗号処理手段905、ハードディスクなどの記憶手段930を有し、バス901に各ブロックが接続されている。

[0219] 情報処理装置900において、情報記録媒体910からMPEG—TSデータからなるAVストリームデータの再生を行う場合、ドライブ909において情報記録媒体910から読み出されたデータは必用に応じて暗号処理手段905で暗号を解きTS・PS処理手段

922によってVideo、Audio、字幕などの各データに分けられる。

[0220] さらに、MPEGコーデック921において復号されたデジタルデータは入出力I／F903内のD／Aコンバータ904によってアナログ信号に変換され出力される。またデジタル出力を行う場合、暗号処理手段905で復号されたMPEG−TSデータは入出力IF902を通してデジタルデータとして出力される。この場合の出力は例えばIEEE1394やイーサネットケーブル、無線LANなどのデジタルインターフェースに対して行われる。なお、ネットワーク接続機能に対応する場合入出力I／F902はネットワーク接続の機能を備える。

[0221] また、情報処理装置900内で出力先機器が受信可能な形式にデータ変換をして出力を行う場合、一旦TS処理手段922で分離したVideo、Audio、字幕などに対してMPEGコーデック921においてレート変換、コーデック変換処理を加え、TS・PS処理手段922で再度MPEG−TSやMPEG−PSなどに多重化を行ったデータをデジタル用入出力I／F902から出力する。または、CPU907の制御の下にMPEG以外のコーデック、多重化ファイルに変換をしてデジタル用入出力I／F902から出力することも可能である。

[0222] CPSユニット管理情報としてのCPSユニット管理テーブル(図2参照)や、CPSユニット対応の再生／コピー制御情報等の管理データは、情報記録媒体910から読み出された後メモリ908に保管される。再生を行う際に必要なCPSユニットごとの鍵情報は、メモリ上に保管されたデータから取得することができる。

[0223] 次に、情報処理装置900が、生成したデータや取得したデータなどの後発データのデータを記録する際の動作について説明する。記録を行うデータとしてデジタル信号入力とアナログ信号入力の2つのケースが想定される。デジタル信号の場合、デジタル信号用入出力I／F902から入力され、必要に応じて暗号処理手段905によって適切な暗号化処理を施したデータを記録媒体910に保存する。

[0224] また、入力されたデジタル信号のデータ形式を変換して保存する場合、MPEGコーデック921およびCPU907、TS・PS処理手段922によって保存用のデータ形式に変換を行い、その後、暗号処理手段905で適切な暗号化処理を施して記録媒体910に保存する。アナログ信号の場合、入出力I／F903へ入力されたアナログ信号は

A／Dコンバータ904によってデジタル信号に変換され、MPEGコーデック921によって記録時に使用されるコーデックへと変換される。

[0225] その後、TS・PS処理手段により、記録データの形式であるAV多重化データへ変換され、必要に応じて暗号処理手段905によって適切な暗号化処理を施したデータが記録媒体910に保存される。なお、コンテンツ管理情報についても記録時に作成し、記録媒体910上に保存する。

[0226] 情報処理装置900において必用な情報を装置外部のネットワーク経由で取得する場合、取得したデータは情報処理装置900内部のメモリ908に保存される。保存されるデータとしてはコンテンツ再生に必用な鍵情報、コンテンツ再生時に合わせて再生するための字幕、Audio、静止画などのデータ、コンテンツ管理情報、およびコンテンツ管理情報に対応した再生装置の動作ルール(Usage Rule)などが存在する。

[0227] なお、再生処理、記録処理を実行するプログラムはROM906内に保管されており、処理中は必要に応じてデータの保管用にメモリ908を使用する。

[0228] 後発データの生成、取得、記録処理について説明する。ドライブ909において情報記録媒体910から実行プログラム、あるいは解析可能なデータを読み込みメモリ908に保持し、CPU907の制御の下にプログラムを実行、またはデータ解析を行う。

[0229] 後発的に生成または取得したデータは、一旦メモリ908に保持され、ユーザの選択、あるいは予め定められた制御シーケンスに従って情報記録媒体910またはハードディスク等の記憶手段930に格納される。

[0230] なお、再生処理、記録処理を実行するプログラムはROM906内に保管されており、プログラムの実行処理中は必要に応じて、パラメータ、データの保管、ワーク領域としてメモリ908を使用する。なお、図21では、データ記録、再生の可能な装置構成を示して説明したが、再生機能のみの装置、記録機能のみを有する装置も構成可能であり、これらの装置においても本発明の適用が可能である。

[0231] 以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特

許請求の範囲の欄を参酌すべきである。

[0232] なお、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。

[0233] 例えば、プログラムは記録媒体としてのハードディスクやROM(Read Only Memory)に予め記録しておくことができる。あるいは、プログラムはフレキシブルディスク、CD−ROM(Compact Disc Read Only Memory), MO(Magneto optical)ディスク, DVD(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納(記録)しておくことができる。このようなリムーバブル記録媒体は、いわゆるパッケージソフトウエアとして提供することができる。

[0234] なお、プログラムは、上述したようなリムーバブル記録媒体からコンピュータにインストールする他、ダウンロードサイトから、コンピュータに無線転送したり、LAN(Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを受信し、内蔵するハードディスク等の記録媒体にインストールすることができる。

[0235] なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。また、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

産業上の利用可能性

[0236] 以上、説明したように、本発明の構成によれば、情報記録媒体に格納されたコンテンツ管理ユニット単位のコンテンツ情報に関連して後発的にユーザが生成した情報やダウンロードした情報などの後発データを、コンテンツ管理ユニットに対応するユニット鍵、または新規のコンテンツ管理ユニットに対応するユニット鍵を適用した暗号化データとして、コンテンツ管理ユニットの構成データとして記録する構成としたので後

発生成データについても、オリジナルのユニット対応データと同様セキュアなデータ管理、利用管理が実現される。従って、後発データの生成や、取得処理を行う構成において、本発明の構成を適用することで、後発データの利用管理を効率的に行なうことが可能となる。

[0237] さらに、本発明の構成によれば、情報記録媒体からの読み取り情報に含まれるプログラムの実行において、プログラムを読み取った情報記録媒体の種類を判定し、予め設定されたプログラム実行の許容された種類であることの確認を条件としてプログラムを実行する構成としたので、例えばコンテンツのコピーディスクを利用したプログラム実行が拒否されることとなり、コンテンツの不正利用を防止することが可能となる。

[0238] さらに、本発明の構成によれば、AVストリームデータファイル以外のナビケーションファイルについても暗号化または改竄検証用データを設定して格納する構成としたので、例えば、PCなど様々なアプリケーションソフトが利用可能な装置において、ライセンスされたアプリケーション以外のアプリケーションを適用してCPSユニット対応のAVストリームデータファイルやナビケーションファイルを利用したり、データ変更を行なうなどの処理を防止することが可能となり、ナビケーションファイルを含むCPSユニット対応データの不正利用の排除が可能となる。

請求の範囲

[1] 情報処理装置であり、

情報記録媒体からのデータ読み取りを実行する記録媒体インタフェースと、

前記情報記録媒体からの取得情報を適用して生成または取得した後発データの記録処理を実行するデータ処理部を有し、

前記情報記録媒体は、各々が異なる暗号鍵として設定されるユニット鍵による暗号化データを含むコンテンツ管理ユニット単位の記録データを格納した情報記録媒体であり、

前記データ処理部は、

前記取得情報の属するコンテンツ管理ユニットに対応するユニット鍵、または新規のコンテンツ管理ユニットに対応するユニット鍵を取得して、取得ユニット鍵を適用した前記後発データの暗号化処理を実行し、生成した暗号化データをコンテンツ管理ユニットの構成データとして記録する処理を実行する構成であることを特徴とする情報処理装置。

[2] 前記データ処理部は、

前記後発データに対応するコンテンツ管理ユニットを設定するとともに、該後発データを含むコンテンツ管理ユニットに対応する管理情報としての暗号鍵の設定処理を実行する構成であることを特徴とする請求項1に記載の情報処理装置。

[3] 前記データ処理部は、

前記後発データに対応するコンテンツ管理ユニットを設定するとともに、該後発データを含むコンテンツ管理ユニットに対応する管理情報としてのコンテンツ利用制御情報の設定処理を実行する構成であることを特徴とする請求項1に記載の情報処理装置。

[4] 前記データ処理部は、

前記情報記録媒体からの取得情報に含まれるプログラムによって規定された領域に対して、前記後発データの書き込み処理を実行する構成であることを特徴とする請求項1に記載の情報処理装置。

[5] 前記データ処理部は、

前記取得情報を取得した情報記録媒体以外の記憶手段に前記後発データを格納する場合において、

前記取得情報を取得した情報記録媒体の識別情報を該後発データに対応付けて格納する処理を実行する構成であることを特徴とする請求項1に記載の情報処理装置。

[6] 前記データ処理部は、

後発データを含むAVストリームデータファイル、およびAVストリームデータの再生処理に適用する制御情報またはプログラムを含むナビケーションファイルの暗号化処理を実行して、記憶手段に対する後発データの記録処理を実行する構成であることを特徴とする請求項1に記載の情報処理装置。

[7] 前記データ処理部は、

前記暗号化処理に適用する暗号鍵として、コンテンツ管理ユニットに対応するユニット鍵を適用する構成であることを特徴とする請求項6に記載の情報処理装置。

[8] 前記データ処理部は、

前記コンテンツ管理ユニットに対する処理を実行するライセンスされたアプリケーションによってのみ取得可能な情報を暗号鍵または暗号鍵生成情報として適用した暗号化処理を実行する構成であることを特徴とする請求項6に記載の情報処理装置。

[9] 前記ライセンスされたアプリケーションによってのみ取得可能な情報は、前記アプリケーションのインストールされたデバイスに固有の識別子としてのデバイスIDを含む情報であることを特徴とする請求項8に記載の情報処理装置。

[10] 前記データ処理部は、

後発データを含むAVストリームデータファイル、およびAVストリームデータの再生処理に適用する制御情報またはプログラムを含むナビケーションファイルの少なくともいずれかのファイルに対して、改竄検証のためのハッシュ値を生成して記憶手段に記録する処理を実行する構成であることを特徴とする請求項1に記載の情報処理装置。

[11] 前記データ処理部は、

後発データを含むAVストリームデータファイルまたはナビケーションファイルの利用

に際して、ファイルに対して設定されたハッシュ値に基づくデータ改竄検証処理を実行し、改竄のないことの確認を条件として各ファイルの利用処理を実行する構成であることを特徴とする請求項10に記載の情報処理装置。

[12] 前記データ処理部は、

後発データを含むAVストリームデータの再生処理に適用する制御情報またはプログラムを含むナビケーションファイルを、改竄検証のための電子署名を付加したファイルとして記憶手段に記録する処理を実行する構成であることを特徴とする請求項1に記載の情報処理装置。

[13] 前記データ処理部は、

後発データを含むAVストリームデータファイルまたはビケーションファイルの利用に際して、ファイルに対して設定された電子署名に基づくデータ改竄検証処理を実行し、改竄のないことの確認を条件として各ファイルの利用処理を実行する構成であることを特徴とする請求項12に記載の情報処理装置。

[14] 情報処理装置であり、

情報記録媒体からのデータ読み取りを実行する記録媒体インタフェースと、

前記情報記録媒体からの読み取り情報に含まれるプログラムの処理を行なうデータ処理部を有し、

前記データ処理部は、

プログラムを読み取った情報記録媒体の種類を判定し、予め設定されたプログラム実行の許容された種類であることの確認を条件としてプログラムを実行する構成であることを特徴とする情報処理装置。

[15] 前記データ処理部は、

プログラム実行の許可される情報記録媒体の種類情報を、前記情報記録媒体からの読み取り情報から取得し、該取得情報に従ってプログラムの実行可否判定を行なう構成であることを特徴とする請求項14に記載の情報処理装置。

[16] 情報処理方法であり、

情報記録媒体からのデータ読み取りを実行するデータ読み取りステップと、

前記情報記録媒体からの取得情報を適用して生成または取得した後発データの

記録処理を実行するデータ処理ステップを有し、

前記情報記録媒体は、各々が異なる暗号鍵として設定されるユニット鍵による暗号化データを含むコンテンツ管理ユニット単位の記録データを格納した情報記録媒体であり、

前記データ処理ステップは、

前記取得情報の属するコンテンツ管理ユニットに対応するユニット鍵、または新規のコンテンツ管理ユニットに対応するユニット鍵を取得するステップと、

取得ユニット鍵を適用した前記後発データの暗号化処理を実行するステップと、

生成した暗号化データをコンテンツ管理ユニットの構成データとして記録する処理を実行するステップと、

を含むことを特徴とする情報処理方法。

[17] 前記データ処理ステップは、

前記後発データに対応するコンテンツ管理ユニットを設定するとともに、該後発データを含むコンテンツ管理ユニットに対応する管理情報としての暗号鍵の設定処理を実行するステップを含むことを特徴とする請求項16に記載の情報処理方法。

[18] 前記データ処理ステップは、

前記後発データに対応するコンテンツ管理ユニットを設定するとともに、該後発データを含むコンテンツ管理ユニットに対応する管理情報としてのコンテンツ利用制御情報の設定処理を実行するステップを含むことを特徴とする請求項16に記載の情報処理方法。

[19] 前記データ処理ステップは、

前記情報記録媒体からの取得情報に含まれるプログラムによって規定された領域に対して、前記後発データの書き込み処理を実行するステップを含むことを特徴とする請求項16に記載の情報処理方法。

[20] 前記データ処理ステップは、

前記取得情報を取得した情報記録媒体以外の記憶手段に前記後発データを格納する場合において、

前記取得情報を取得した情報記録媒体の識別情報を該後発データに対応付けて

格納する処理を実行することを特徴とする請求項16に記載の情報処理方法。

[21] 前記情報処理方法は、さらに、

後発データを含むAVストリームデータファイル、およびAVストリームデータの再生処理に適用する制御情報またはプログラムを含むナビケーションファイルの暗号化処理を実行して、記憶手段に記録する処理を実行する暗号化記録処理ステップを含むことを特徴とする請求項16に記載の情報処理方法。

[22] 前記暗号化記録処理ステップは、

コンテンツ管理ユニットに対応するユニット鍵を暗号鍵として適用した暗号化処理を実行するステップであることを特徴とする請求項21に記載の情報処理方法。

[23] 前記暗号化記録処理ステップは、

前記コンテンツ管理ユニットに対する処理を実行するライセンスされたアプリケーションによってのみ取得可能な情報を暗号鍵または暗号鍵生成情報として適用した暗号化処理を実行するステップであることを特徴とする請求項21に記載の情報処理方法。

[24] 前記ライセンスされたアプリケーションによってのみ取得可能な情報は、前記アプリケーションのインストールされたデバイスに固有の識別子としてのデバイスIDを含む情報であることを特徴とする請求項23に記載の情報処理方法。

[25] 前記情報処理方法は、さらに、

後発データを含むAVストリームデータファイル、およびAVストリームデータの再生処理に適用する制御情報またはプログラムを含むナビケーションファイルの少なくともいずれかのファイルに対して、改竄検証のためのハッシュ値を生成して記憶手段に記録する処理を実行するステップを有することを特徴とする請求項16に記載の情報処理方法。

[26] 前記情報処理方法は、さらに、

後発データを含むAVストリームデータファイルまたはナビケーションファイルの利用に際して、ファイルに対して設定されたハッシュ値に基づくデータ改竄検証処理を実行し、改竄のないことの確認を条件として各ファイルの利用処理を実行するステップを有することを特徴とする請求項25に記載の情報処理方法。

[27] 前記情報処理方法は、さらに、

後発データを含むAVストリームデータの再生処理に適用する制御情報またはプログラムを含むナビケーションファイルを、改竄検証のための電子署名を付加したファイルとして記憶手段に記録する処理を実行するステップを有することを特徴とする請求項16に記載の情報処理方法。

[28] 前記情報処理方法は、さらに、

後発データを含むAVストリームデータファイルまたはビケーションファイルの利用に際して、ファイルに対して設定された電子署名に基づくデータ改竄検証処理を実行し、改竄のないことの確認を条件として各ファイルの利用処理を実行するステップを有することを特徴とする請求項27に記載の情報処理方法。

[29] 情報処理方法であり、

情報記録媒体からのデータ読み取りを実行するデータ読み取りステップと、

前記情報記録媒体からの読み取り情報に含まれるプログラムの処理を行なうデータ処理ステップを有し、

-前記データ処理ステップは、

プログラムを読み取った情報記録媒体の種類を判定し、予め設定されたプログラム実行の許容された種類であることの確認を条件としてプログラムを実行するステップを含むことを特徴とする情報処理方法。

[30] 前記データ処理ステップにおいて、プログラム実行の許可される情報記録媒体の種類情報を、前記情報記録媒体からの読み取り情報から取得し、該取得情報に従ってプログラムの実行可否判定を行なうことを特徴とする請求項29に記載の情報処理方法。

[31] 情報処理を実行するコンピュータ・プログラムであり、

情報記録媒体からのデータ読み取りを実行するデータ読み取りステップと、

前記情報記録媒体からの取得情報を適用して生成または取得した後発データの記録処理を実行するデータ処理ステップを有し、

前記情報記録媒体は、各々が異なる暗号鍵として設定されるユニット鍵による暗号化データを含むコンテンツ管理ユニット単位の記録データを格納した情報記録媒体

であり、

前記データ処理ステップは、

前記取得情報の属するコンテンツ管理ユニットに対応するユニット鍵、または新規のコンテンツ管理ユニットに対応するユニット鍵を取得するステップと、

取得ユニット鍵を適用した前記後発データの暗号化処理を実行するステップと、

生成した暗号化データをコンテンツ管理ユニットの構成データとして記録する処理を実行するステップと、

を含むことを特徴とするコンピュータ・プログラム。

[32] 前記コンピュータ・プログラムは、さらに、

後発データを含むAVストリームデータファイル、およびAVストリームデータの再生処理に適用する制御情報またはプログラムを含むナビケーションファイルの暗号化処理を実行して記憶手段に記録する処理を実行する暗号化記録処理ステップを有することを特徴とする請求項31に記載のコンピュータ・プログラム。

[33] 前記コンピュータ・プログラムは、さらに、

後発データを含むAVストリームデータファイル、およびAVストリームデータの再生処理に適用する制御情報またはプログラムを含むナビケーションファイルの少なくともいずれかのファイルに対する改竄検証用データを記憶手段に記録する処理を実行するステップを有することを特徴とする請求項31に記載のコンピュータ・プログラム。

[34] 前記コンピュータ・プログラムは、さらに、

後発データを含むAVストリームデータファイルまたはナビケーションファイルの利用に際して、ファイルに対して設定された改竄検証用データに基づくデータ改竄検証処理を実行し、改竄のないことの確認を条件として各ファイルの利用処理を実行するステップを有することを特徴とする請求項31に記載のコンピュータ・プログラム。

[35] 情報処理を実行するコンピュータ・プログラムであり、

情報記録媒体からのデータ読み取りを実行するデータ読み取りステップと、

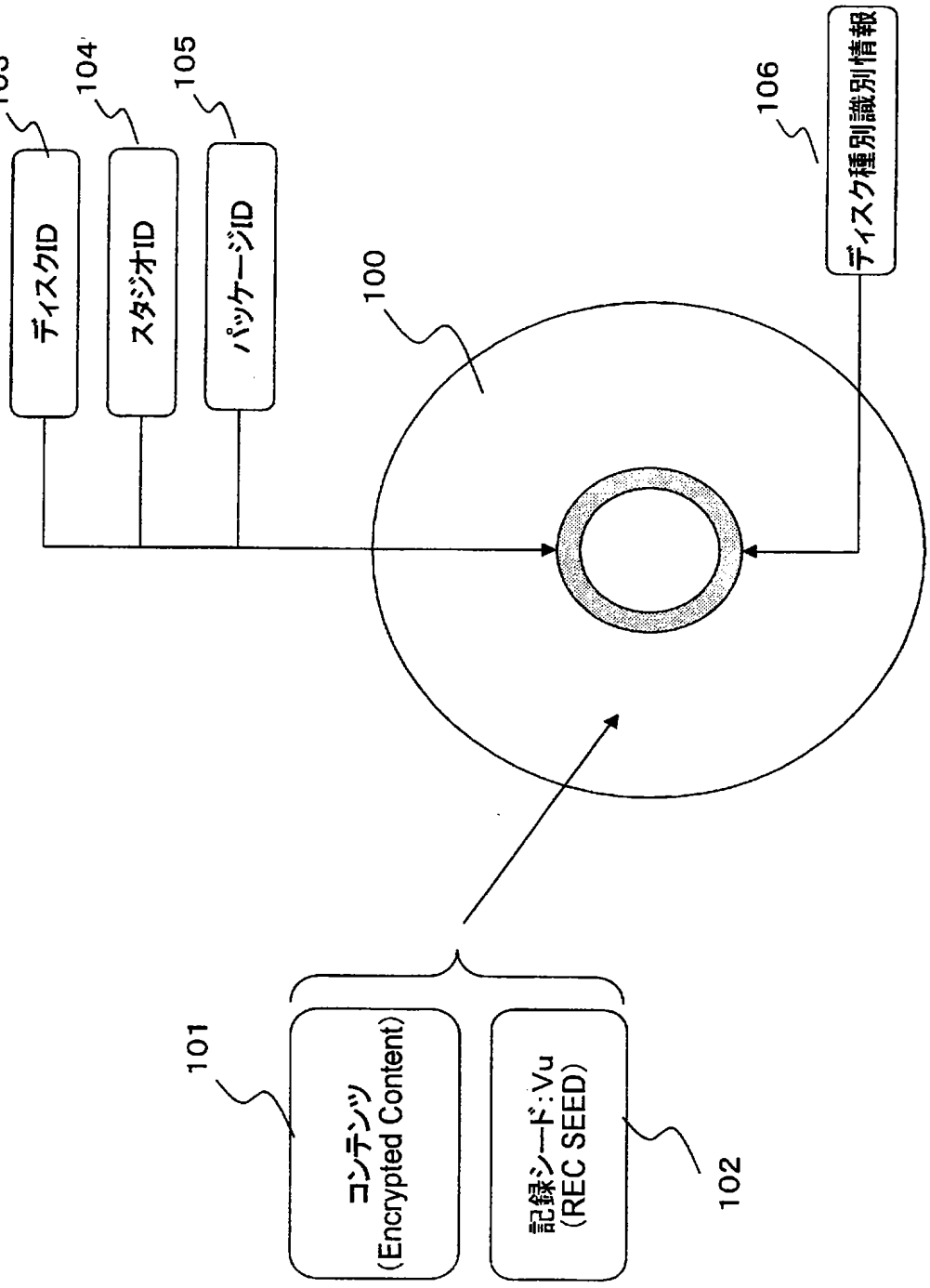
前記情報記録媒体からの読み取り情報に含まれるプログラムの処理を行なうデータ処理ステップを有し、

前記データ処理ステップは、

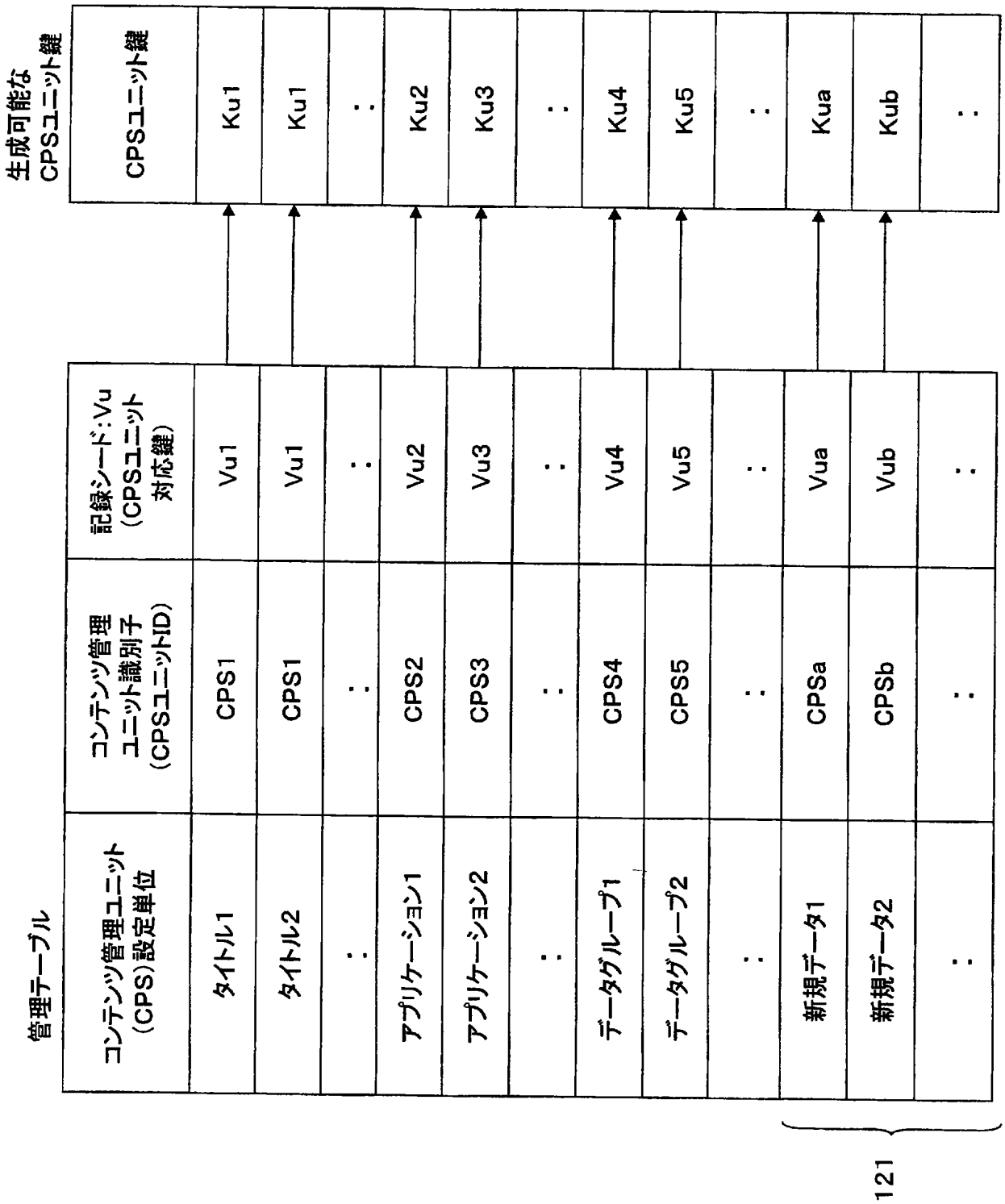
プログラムを読み取った情報記録媒体の種類を判定し、予め設定されたプログラム実行の許容された種類であることの確認を条件としてプログラムを実行するステップを含むことを特徴とするコンピュータ・プログラム。

WO 2005/074187 PCT/JP2005/001147

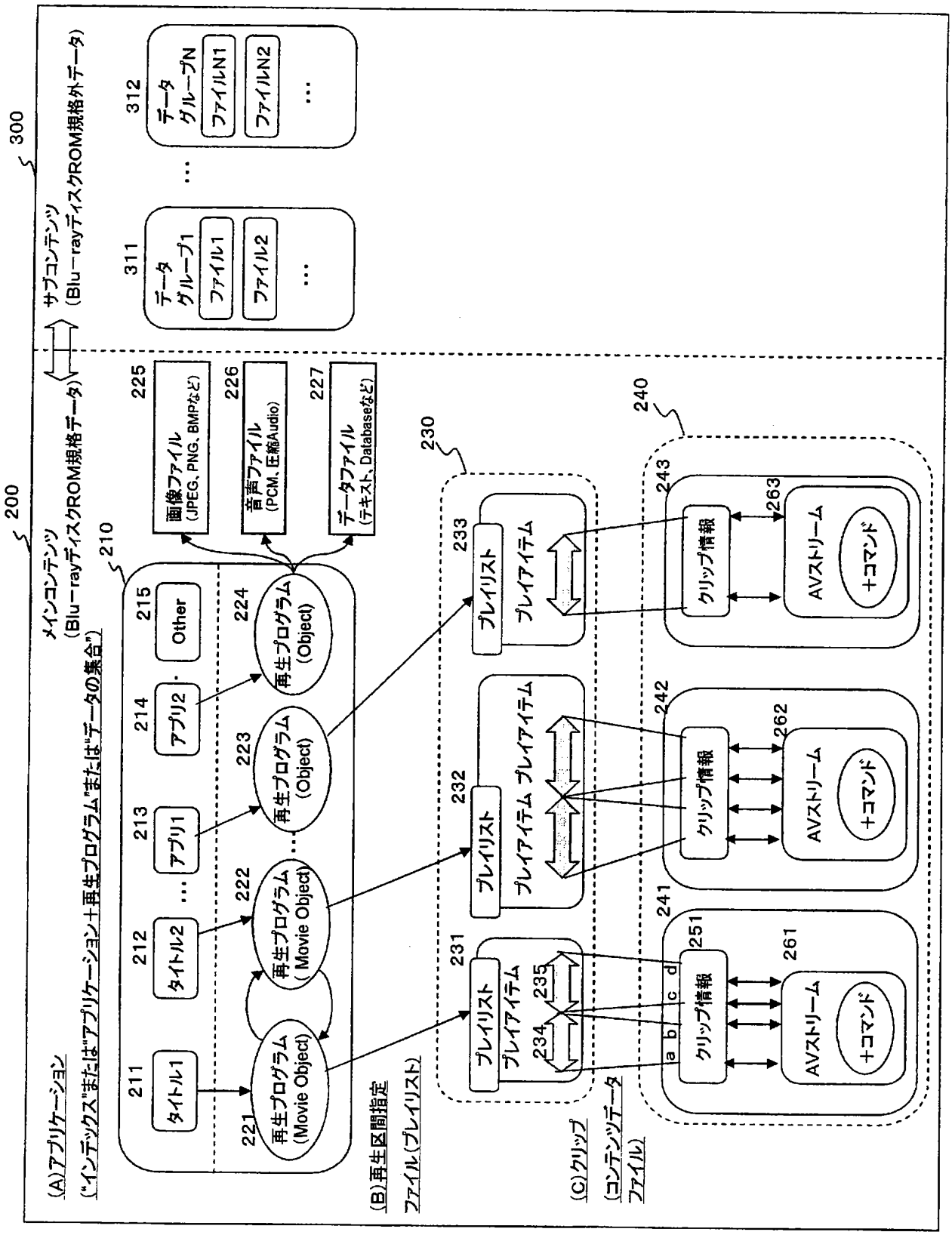
[図1]



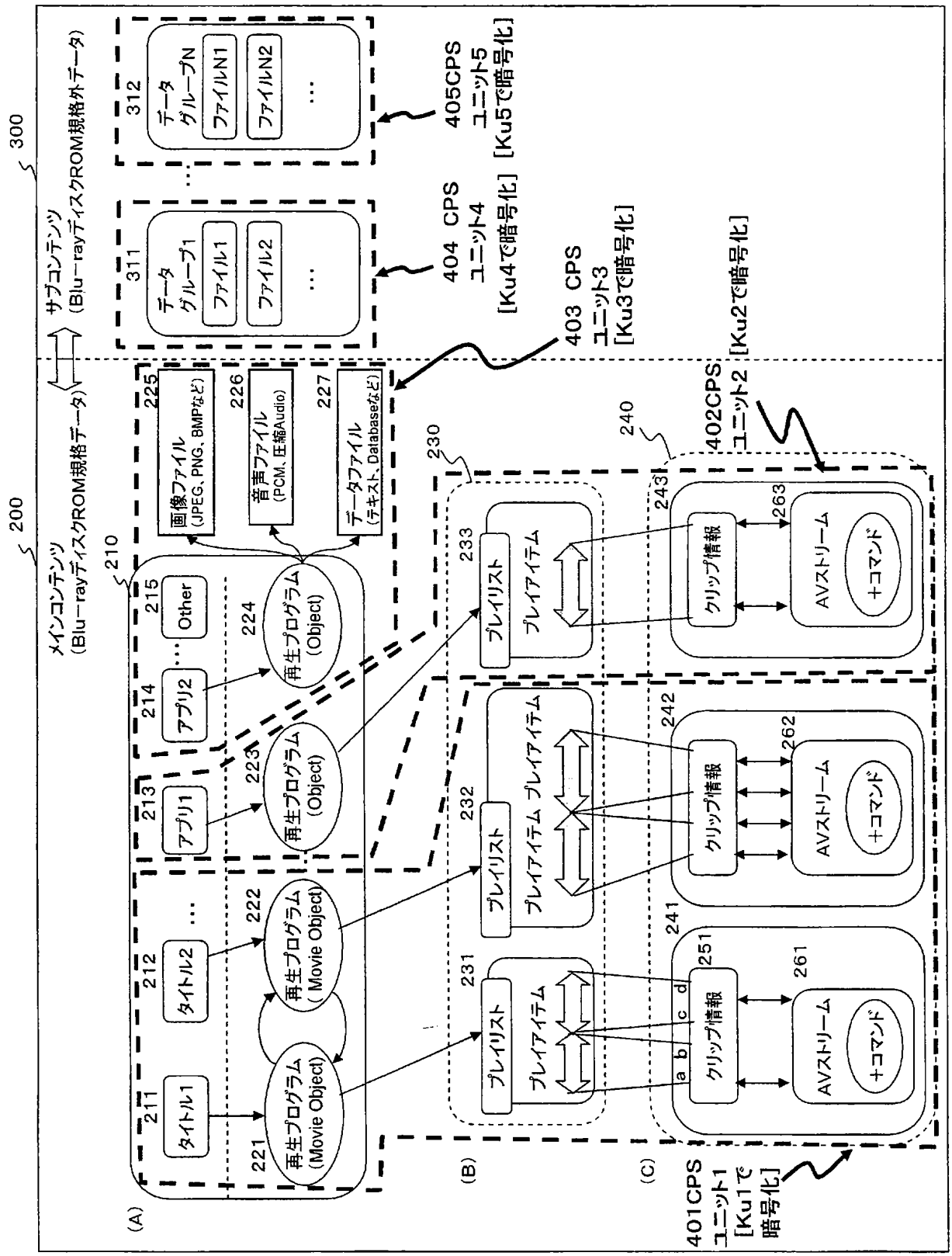
[図2]


管理テーブル
コンテンツ管理ユニット(CPS)設定単位
コンテンツ管理ユニット識別子(CPSユニットID)
記録シード:Vu(CPSユニット対応鍵)
生成可能なCPSユニット鍵
CPSユニット鍵
タイトル1
CPS1
Vu1
Ku1
タイトル2
CPS1
Vu1
Ku1
アプリケーション1
CPS2
Vu2
Ku2
アプリケーション2
CPS3
Vu3
Ku3
データグループ1
CPS4
Vu4
Ku4
データグループ2
CPS5
Vu5
Ku5
新規データ1
CPSa
Vua
Kua
新規データ2
CPSb
Vub
Kub
121

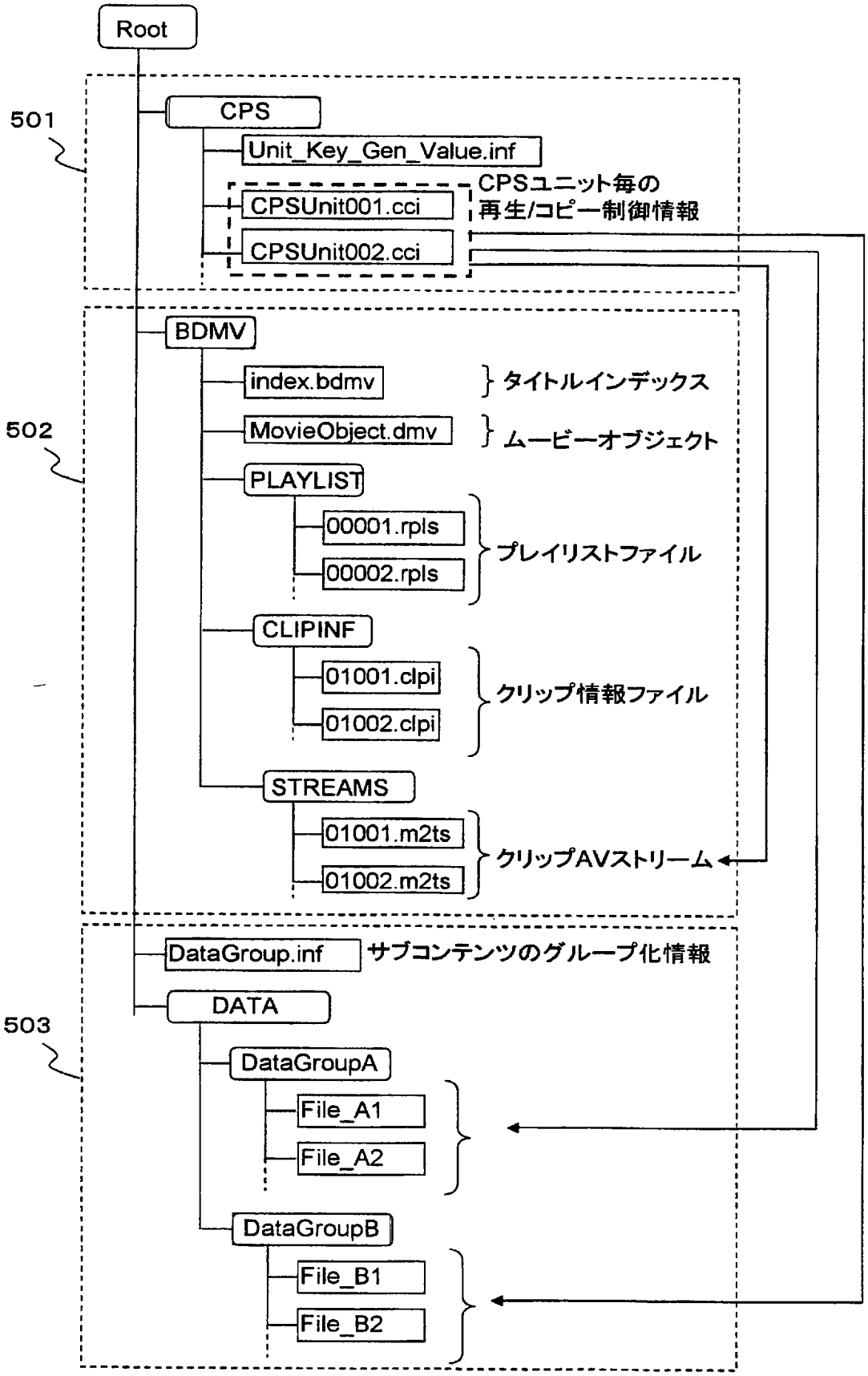
[図3]


300
メインコンテンツ
(Blu-rayディスクROM規格データ)
サブコンテンツ
(Blu-rayディスクROM規格外データ)
200
(A)アプリケーション
("インデックス"または"アプリケーション+再生プログラム"または"データの集合")
210
211
タイトル1
212
タイトル2
213
アプリ1
214
アプリ2
215
Other
221
再生プログラム
(Movie Object)
222
再生プログラム
(Movie Object)
223
再生プログラム
(Object)
224
再生プログラム
(Object)
225
画像ファイル
(JPEG、PNG、BMPなど)
226
音声ファイル
(PCM、圧縮Audio)
227
データファイル
(テキスト、Databaseなど)
311
データ
グループ1
ファイル1
ファイル2
312
データ
グループN
ファイルN1
ファイルN2
(B)再生区間指定
ファイル(プレイリスト)
230
231
プレイリスト
プレイアイテム
234
235
232
プレイリスト
プレイアイテム
233
プレイリスト
プレイアイテム
(C)クリップ
(コンテンツデータ
ファイル)
240
241
a
b
c
d
251
クリップ情報
261
AVストリーム
+コマンド
242
クリップ情報
262
AVストリーム
+コマンド
243
クリップ情報
263
AVストリーム
+コマンド

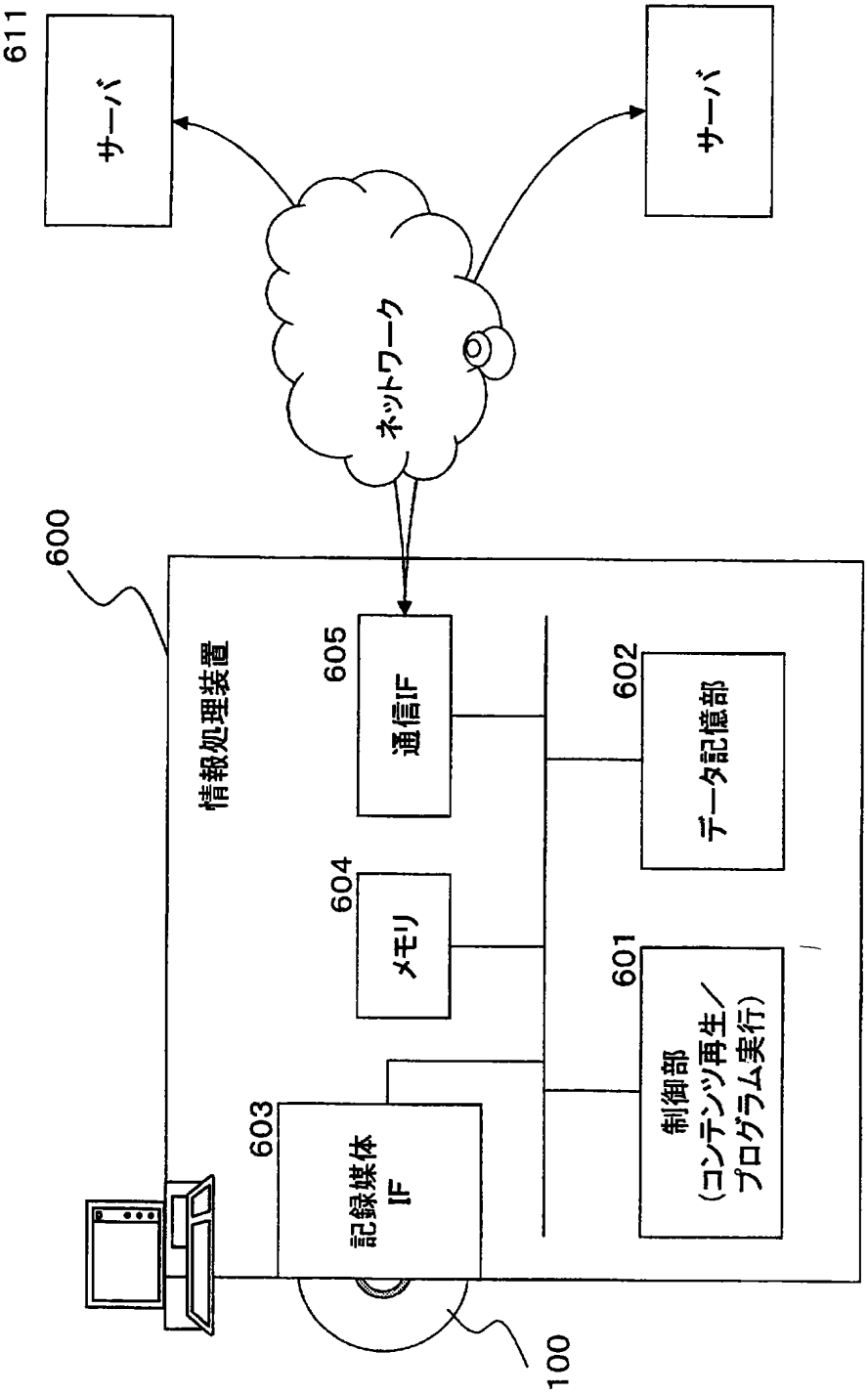
[図4]


300
200
メインコンテンツ
(Blu-rayディスクROM規格データ)
サブコンテンツ
(Blu-rayディスクROM規格外データ)
210
211
タイトル1
212
タイトル2
213
アプリ1
214
アプリ2
215
Other
221
再生プログラム
(Movie Object)
222
再生プログラム
(Movie Object)
223
再生プログラム
(Object)
224
再生プログラム
(Object)
225
画像ファイル
(JPEG、PNG、BMPなど)
226
音声ファイル
(PCM、圧縮Audio)
227
データファイル
(テキスト、Databaseなど)
311
データ
グループ1
ファイル1
ファイル2
312
データ
グループN
ファイルN1
ファイルN2
404 CPS
ユニット4
[Ku4で暗号化]
405CPS
ユニット5
[Ku5で暗号化]
403 CPS
ユニット3
[Ku3で暗号化]
402CPS
ユニット2 [Ku2で暗号化]
401CPS
ユニット1
[Ku1で
暗号化]
(A)
(B)
(C)
230
231
プレイリスト
プレイアイテム
232
プレイリスト
プレイアイテム プレイアイテム
233
プレイリスト
プレイアイテム
240
241
a b c d
クリップ情報
251
AVストリーム
+コマンド
261
242
クリップ情報
AVストリーム
+コマンド
262
243
クリップ情報
AVストリーム
+コマンド
263

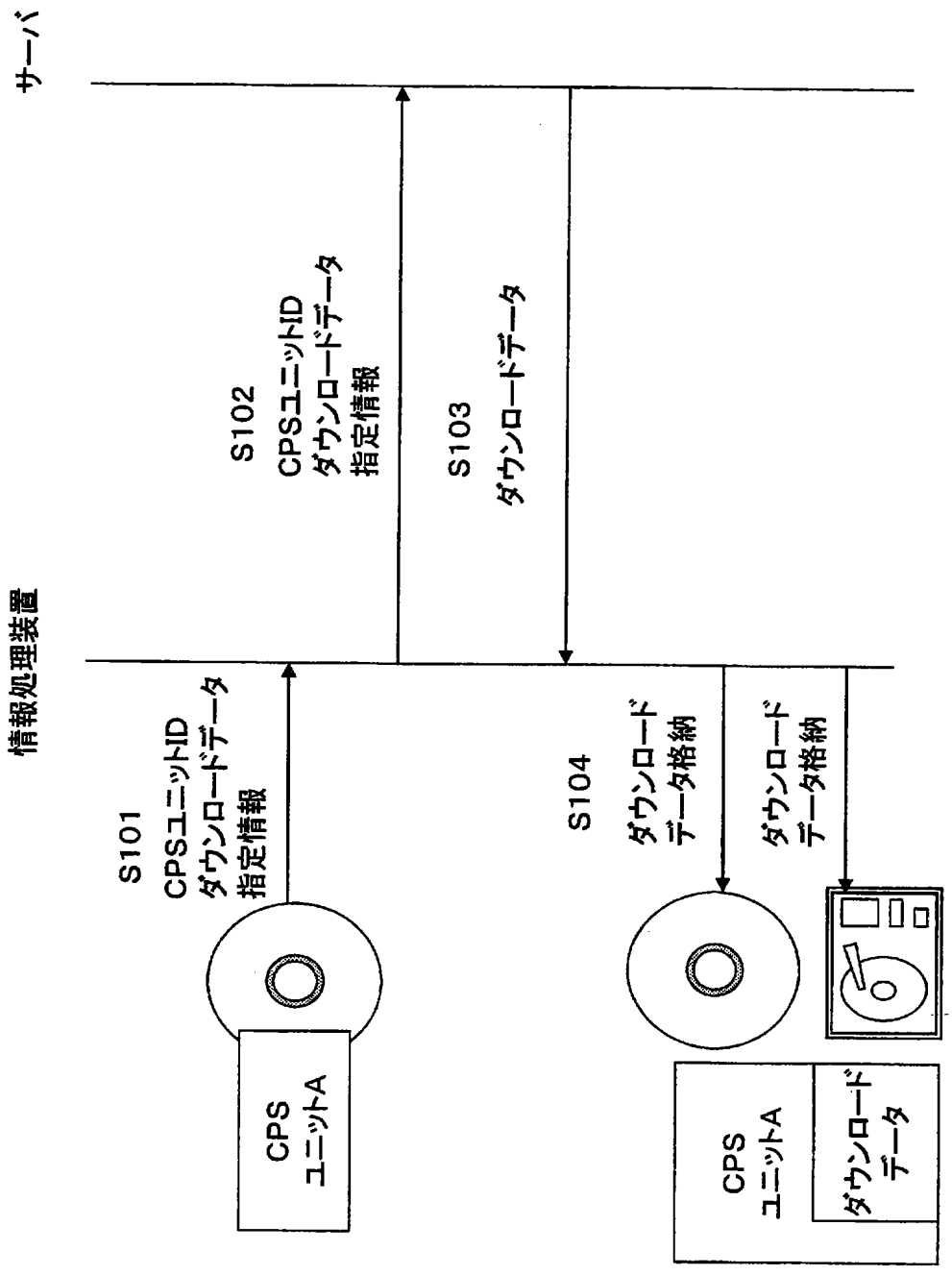
[図5]


Root
501
CPS
Unit_Key_Gen_Value.inf
CPSユニット毎の
再生/コピー制御情報
CPSUnit001.cci
CPSUnit002.cci
BDMV
index.bdmv
タイトルインデックス
502
MovieObject.dmv
ムービーオブジェクト
PLAYLIST
00001.rpls
00002.rpls
プレイリストファイル
CLIPINF
01001.clpi
01002.clpi
クリップ情報ファイル
STREAMS
01001.m2ts
01002.m2ts
クリップAVストリーム
DataGroup.inf
サブコンテンツのグループ化情報
503
DATA
DataGroupA
File_A1
File_A2
DataGroupB
File_B1
File_B2

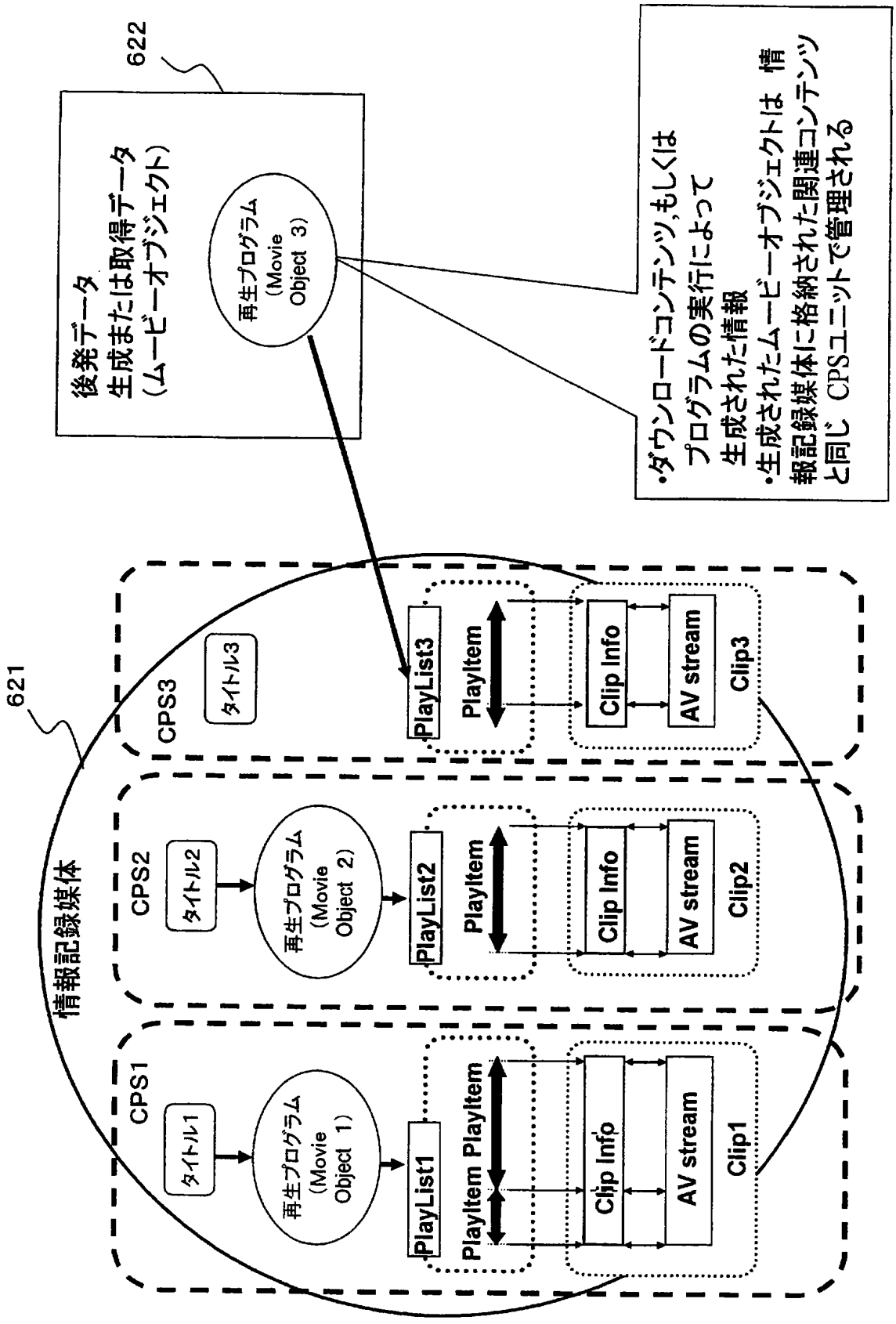
[図6]


611
サーバ
サーバ
ネットワーク
600
情報処理装置
605
通信IF
602
データ記憶部
604
メモリ
601
制御部
(コンテンツ再生／
プログラム実行)
603
記録媒体
IF
100

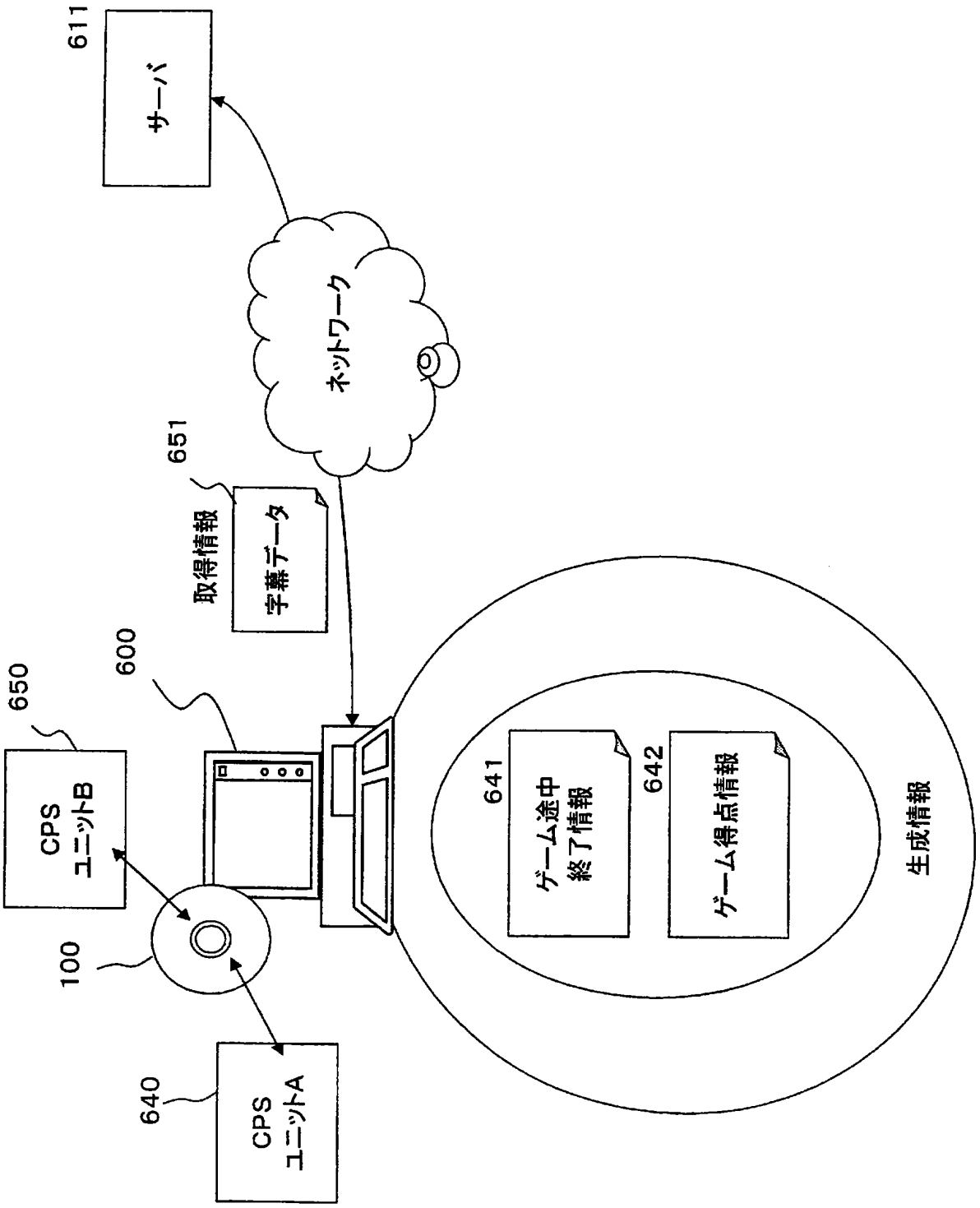
[図7]


サーバ
情報処理装置
S101
CPSユニットID
ダウンロードデータ
指定情報
S102
CPSユニットID
ダウンロードデータ
指定情報
S103
ダウンロードデータ
S104
ダウンロード
データ格納
ダウンロード
データ格納
CPS
ユニットA
CPS
ユニットA
ダウンロード
データ

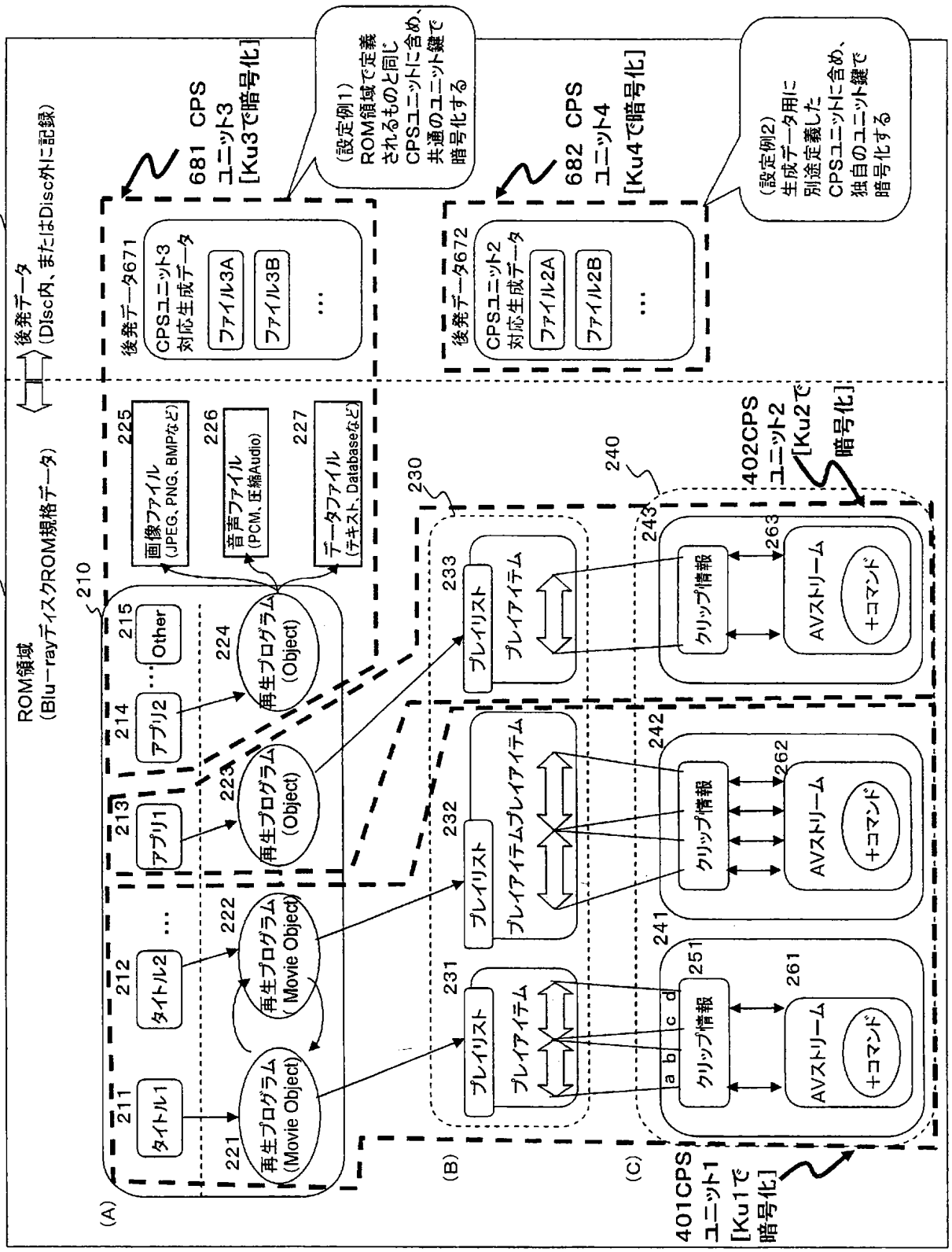
[図8]


622
後発データ
生成または取得データ
(ムービーオブジェクト)
再生プログラム
(Movie
Object 3)
•ダウンロードコンテンツ,もしくは
プログラムの実行によって
生成された情報
•生成されたムービーオブジェクトは 情
報記録媒体に格納された関連コンテンツ
と同じ CPSユニットで管理される
621
情報記録媒体
CPS3
タイトル3
PlayList3
PlayItem
Clip Info
AV stream
Clip3
CPS2
タイトル2
再生プログラム
(Movie
Object 2)
PlayList2
PlayItem
Clip Info
AV stream
Clip2
CPS1
タイトル1
再生プログラム
(Movie
Object 1)
PlayList1
PlayItem PlayItem
Clip Info
AV stream
Clip1

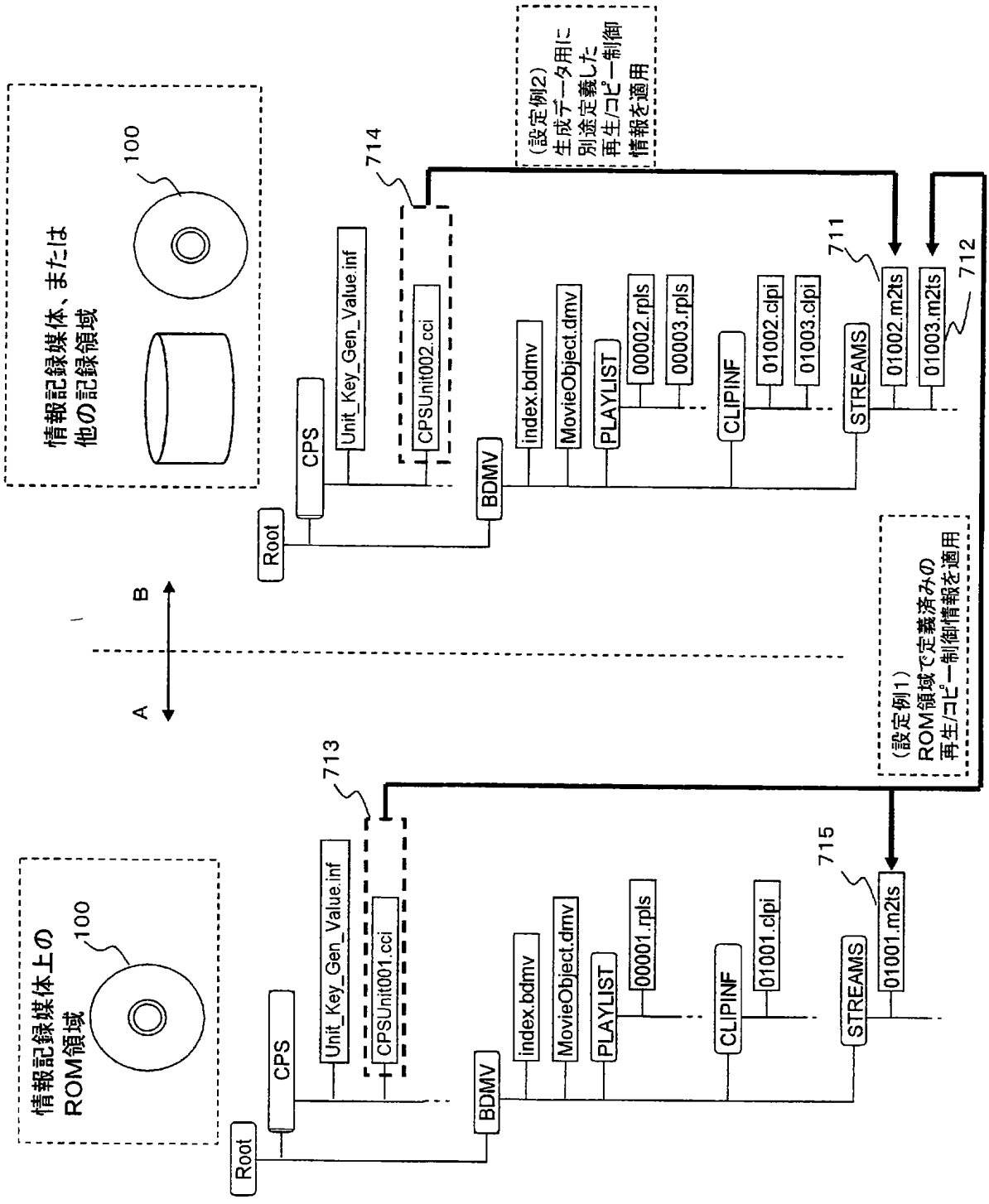
[図9]


611
サーバ
ネットワーク
651
取得情報
字幕データ
600
650
CPS
ユニットB
100
640
CPS
ユニットA
641
ゲーム途中
終了情報
642
ゲーム得点情報
生成情報

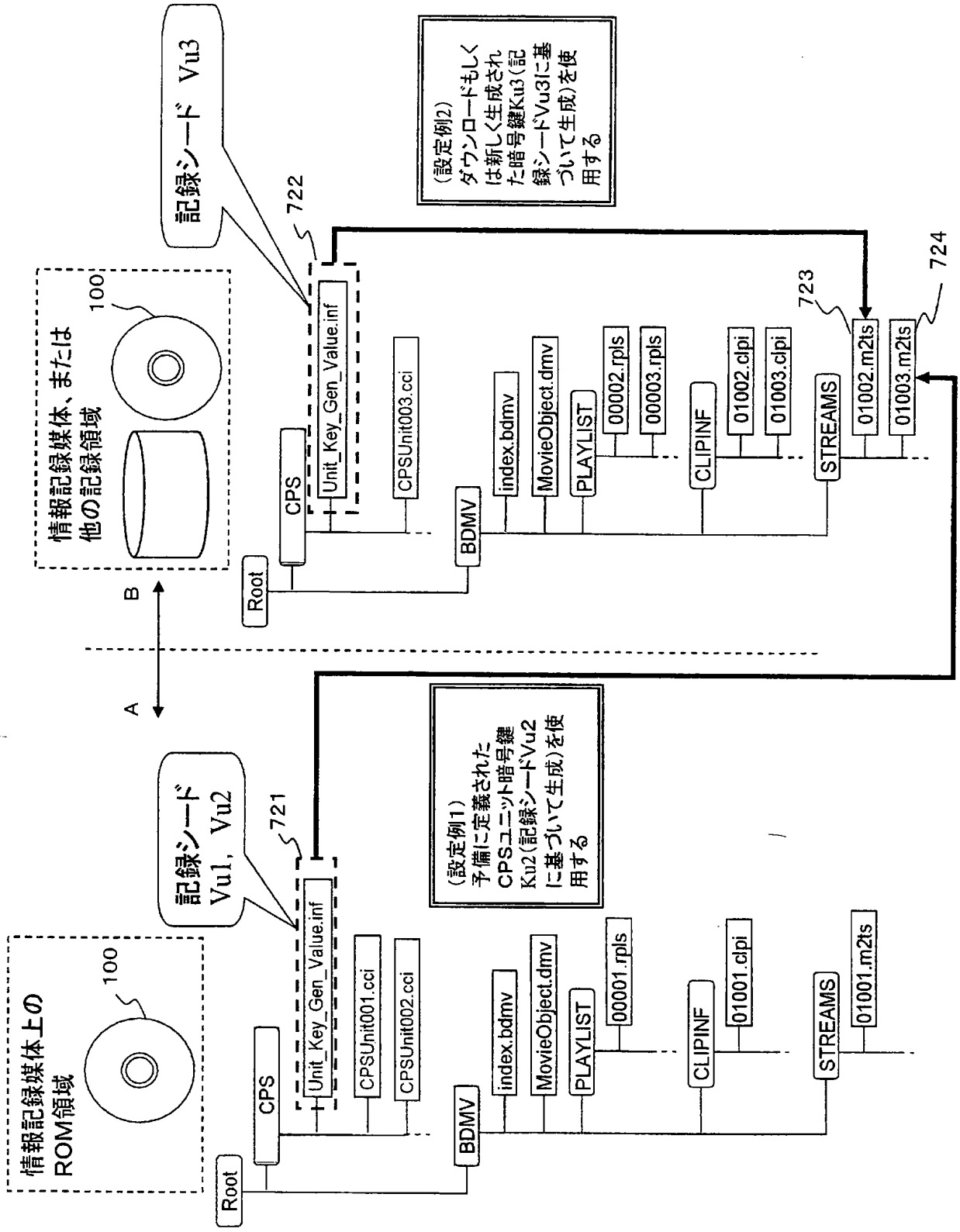
[図10]


670
後発データ
(DIsc内、またはDisc外に記録)
660
ROM領域
(Blu-rayディスクROM規格データ)
210
211
タイトル1
212
タイトル2
213
アプリ1
214
アプリ2
215
Other
221
再生プログラム
(Movie Object)
222
再生プログラム
(Movie Object)
223
再生プログラム
(Object)
224
再生プログラム
(Object)
225
画像ファイル
(JPEG、PNG、BMPなど)
226
音声ファイル
(PCM、圧縮Audio)
227
データファイル
(テキスト、Databaseなど)
後発データ9671
CPSユニット3
対応生成データ
ファイル3A
ファイル3B
...
681 CPS
ユニット3
[Ku3で暗号化]
(設定例1)
ROM領域で定義
されるものと同じ
CPSユニットに含め、
共通のユニット鍵で
暗号化する
後発データ9672
CPSユニット2
対応生成データ
ファイル2A
ファイル2B
...
682 CPS
ユニット4
[Ku4で暗号化]
(設定例2)
生成データ用に
別途定義した
CPSユニットに含め、
独自のユニット鍵で
暗号化する
402CPS
ユニット2
[Ku2で
暗号化]
(A)
(B)
(C)
230
231
プレイリスト
プレイアイテム
232
プレイリスト
プレイアイテムプレイアイテム
233
プレイリスト
プレイアイテム
240
241
a b c d
251
クリップ情報
261
AVストリーム
+コマンド
242
クリップ情報
262
AVストリーム
+コマンド
243
クリップ情報
263
AVストリーム
+コマンド
401CPS
ユニット1
[Ku1で
暗号化]

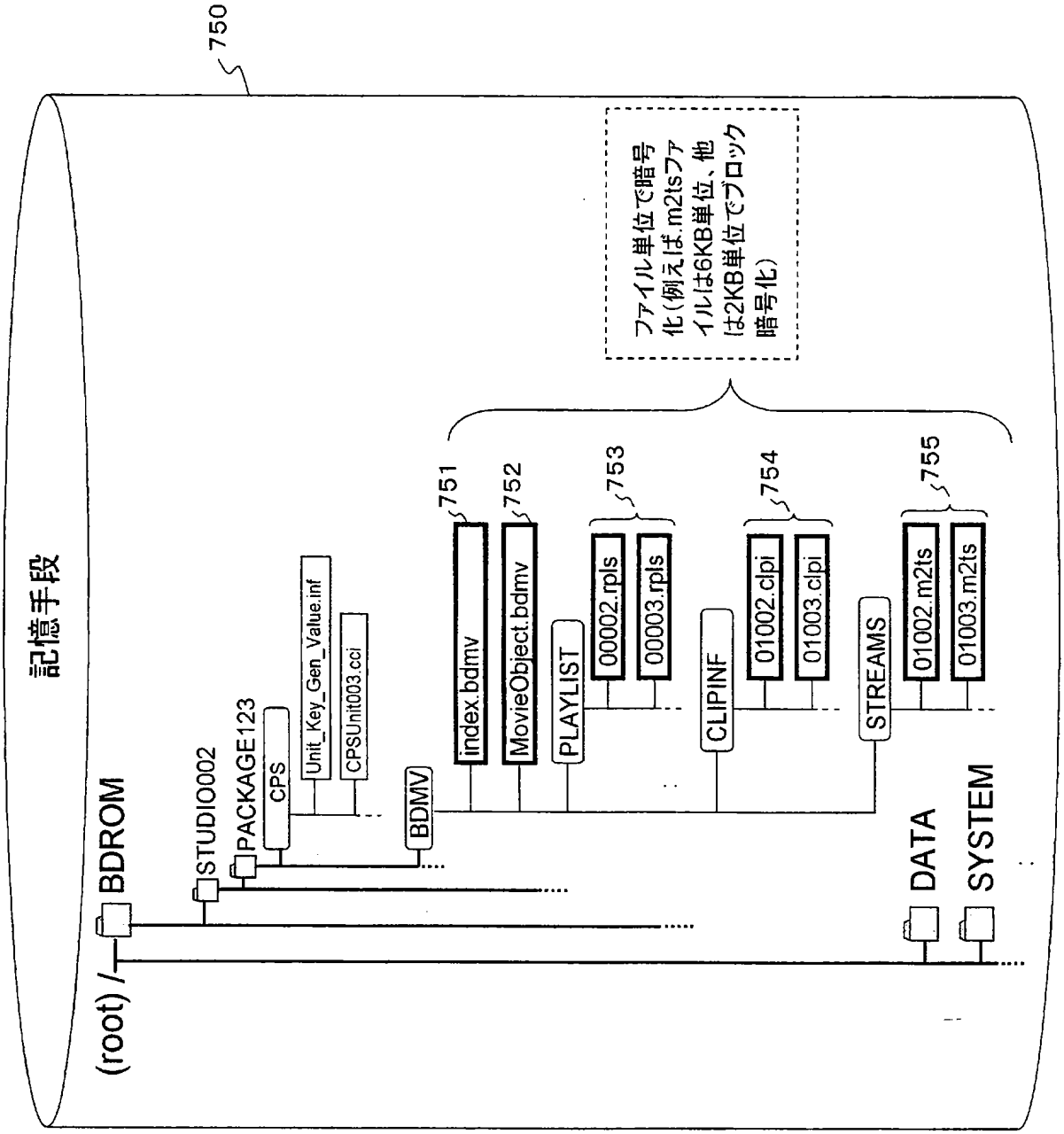
[図11]


情報記録媒体上の
ROM領域
100
Root
CPS
Unit_Key_Gen_Value.inf
CPSUnit001.cci
713
BDMV
index.bdmv
MovieObject.dmv
PLAYLIST
00001.rpls
CLIPINF
01001.clpi
STREAMS
01001.m2ts
715
A
B
情報記録媒体、または
他の記録領域
100
Root
CPS
Unit_Key_Gen_Value.inf
CPSUnit002.cci
714
BDMV
index.bdmv
MovieObject.dmv
PLAYLIST
00002.rpls
00003.rpls
CLIPINF
01002.clpi
01003.clpi
STREAMS
01002.m2ts
01003.m2ts
711
712
(設定例2)
生成データ用に
別途定義した
再生/コピー制御
情報を適用
(設定例1)
ROM領域で定義済みの
再生/コピー制御情報を適用

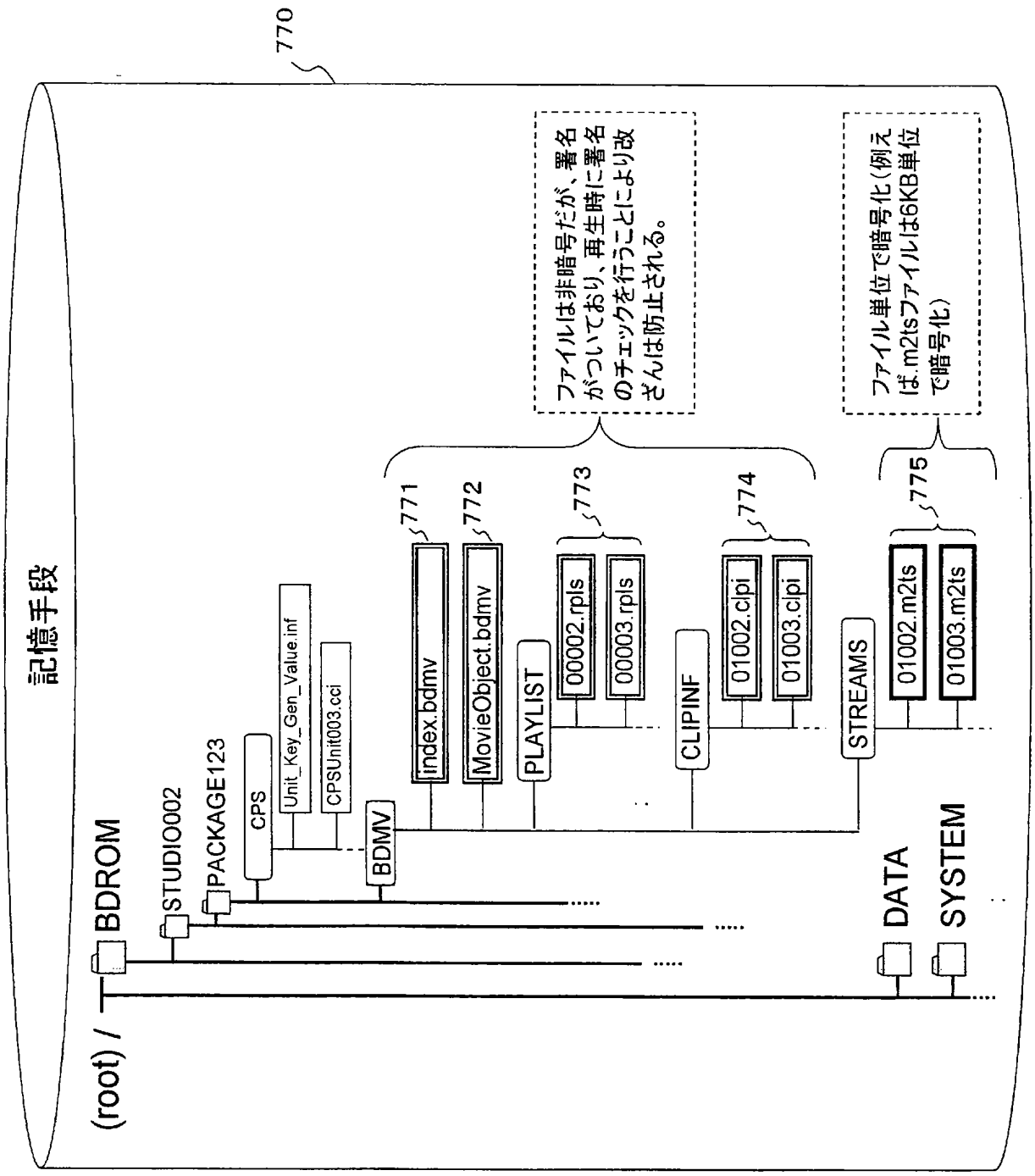
[図12]


情報記録媒体上の
ROM領域
100
記録シード
Vu1, Vu2
721
Root
CPS
Unit_Key_Gen_Value.inf
CPSUnit001.cci
CPSUnit002.cci
BDMV
index.bdmv
MovieObject.dmv
PLAYLIST
00001.rpls
CLIPINF
01001.clpi
STREAMS
01001.m2ts
(設定例1)
予備に定義された
CPSユニット暗号鍵
Ku2(記録シードVu2
に基づいて生成)を使
用する
A
B
情報記録媒体、または
他の記録領域
100
記録シード Vu3
722
Root
CPS
Unit_Key_Gen_Value.inf
CPSUnit003.cci
BDMV
index.bdmv
MovieObject.dmv
PLAYLIST
00002.rpls
00003.rpls
CLIPINF
01002.clpi
01003.clpi
STREAMS
01002.m2ts
01003.m2ts
723
724
(設定例2)
ダウンロードもしく
は新しく生成され
た暗号鍵Ku3(記
録シードVu3に基
づいて生成)を使
用する

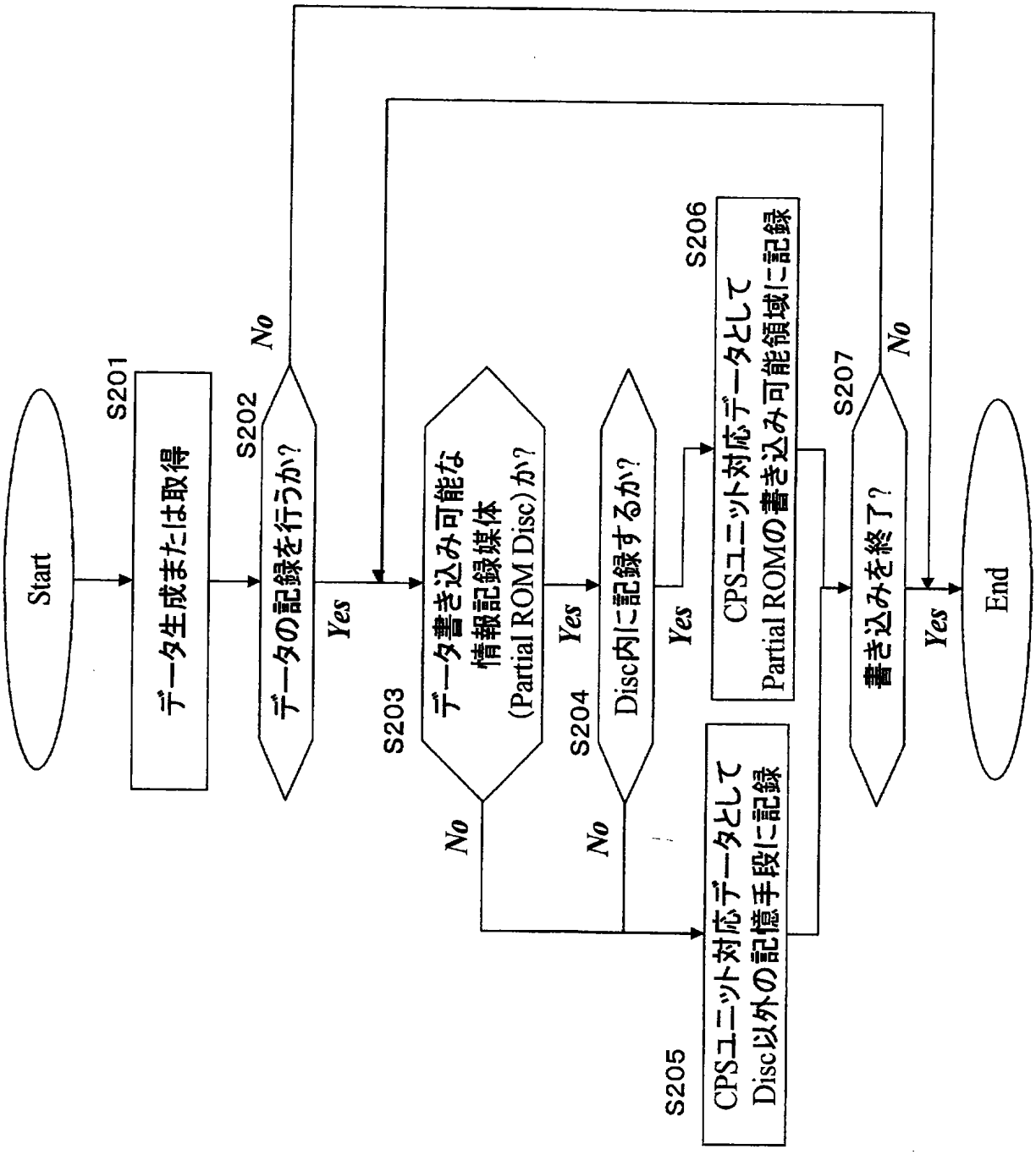
[図13]


750
記憶手段
(root)
BDROM
STUDIO002
PACKAGE123
CPS
Unit_Key_Gen_Value.inf
CPSUnit003.cci
BDMV
751
index.bdmv
752
MovieObject.bdmv
PLAYLIST
753
00002.rpls
00003.rpls
CLIPINF
754
01002.clpi
01003.clpi
STREAMS
755
01002.m2ts
01003.m2ts
DATA
SYSTEM
ファイル単位で暗号化（例えば.m2tsファイルは6KB単位、他は2KB単位でブロック暗号化）

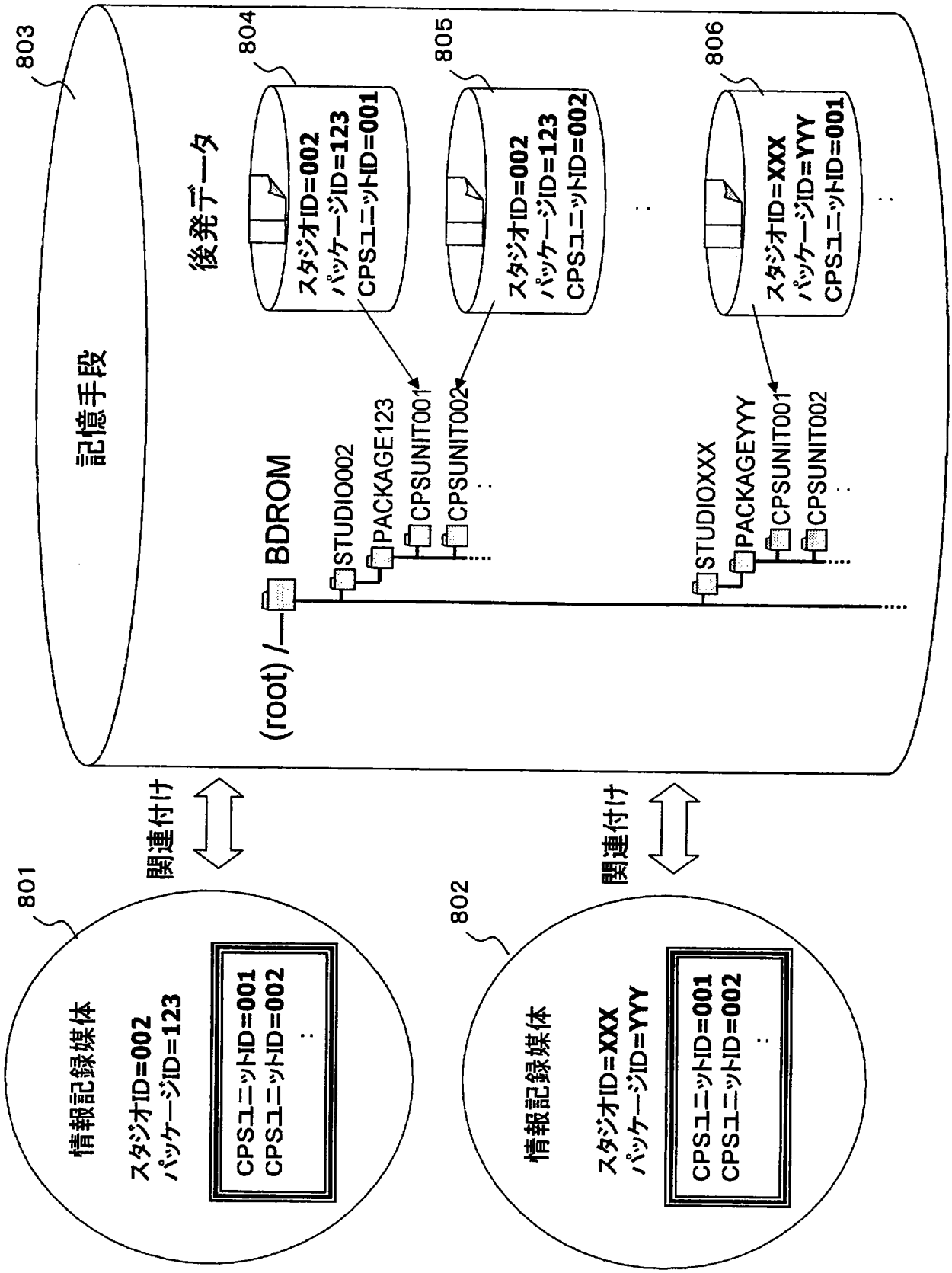
[図14]


770
記憶手段
(root) /
BDROM
STUDIO002
PACKAGE123
CPS
Unit_Key_Gen_Value.inf
CPSUnit003.cci
BDMV
index.bdmv
MovieObject.bdmv
PLAYLIST
00002.rpls
00003.rpls
CLIPINF
01002.clpi
01003.clpi
STREAMS
01002.m2ts
01003.m2ts
DATA
SYSTEM
771
772
773
774
775
ファイルは非暗号だが、署名がついており、再生時に署名のチェックを行うことにより改ざんは防止される。
ファイル単位で暗号化（例えば.m2tsファイルは6KB単位で暗号化）

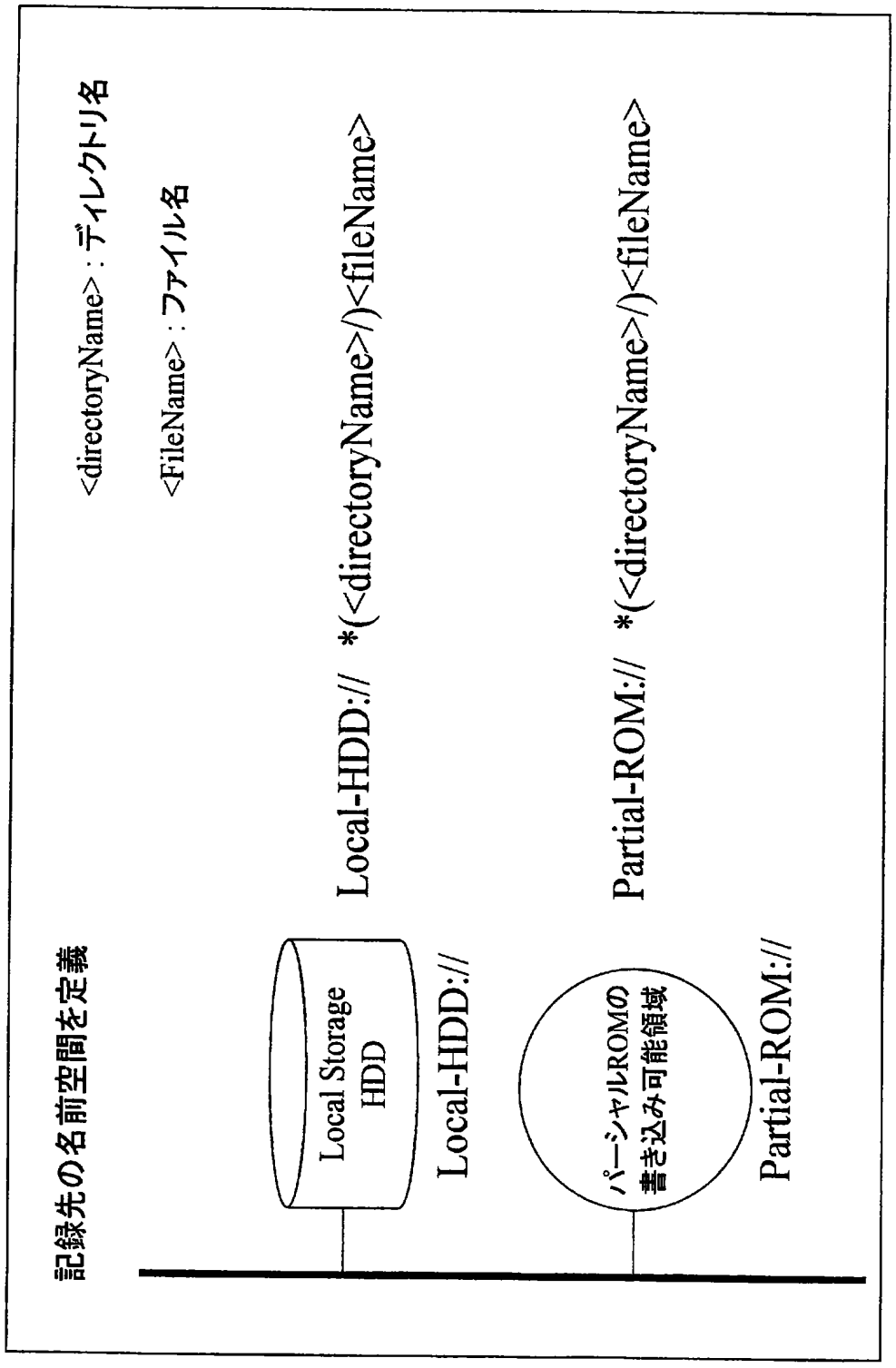
[図15]


Start
S201
データ生成または取得
S202
データの記録を行うか?
No
Yes
S203
データ書き込み可能な
情報記録媒体
(Partial ROM Disc)か?
No
Yes
S204
Disc内に記録するか?
No
Yes
S205
CPSユニット対応データとして
Disc以外の記憶手段に記録
S206
CPSユニット対応データとして
Partial ROMの書き込み可能領域に記録
S207
書き込みを終了?
No
Yes
End

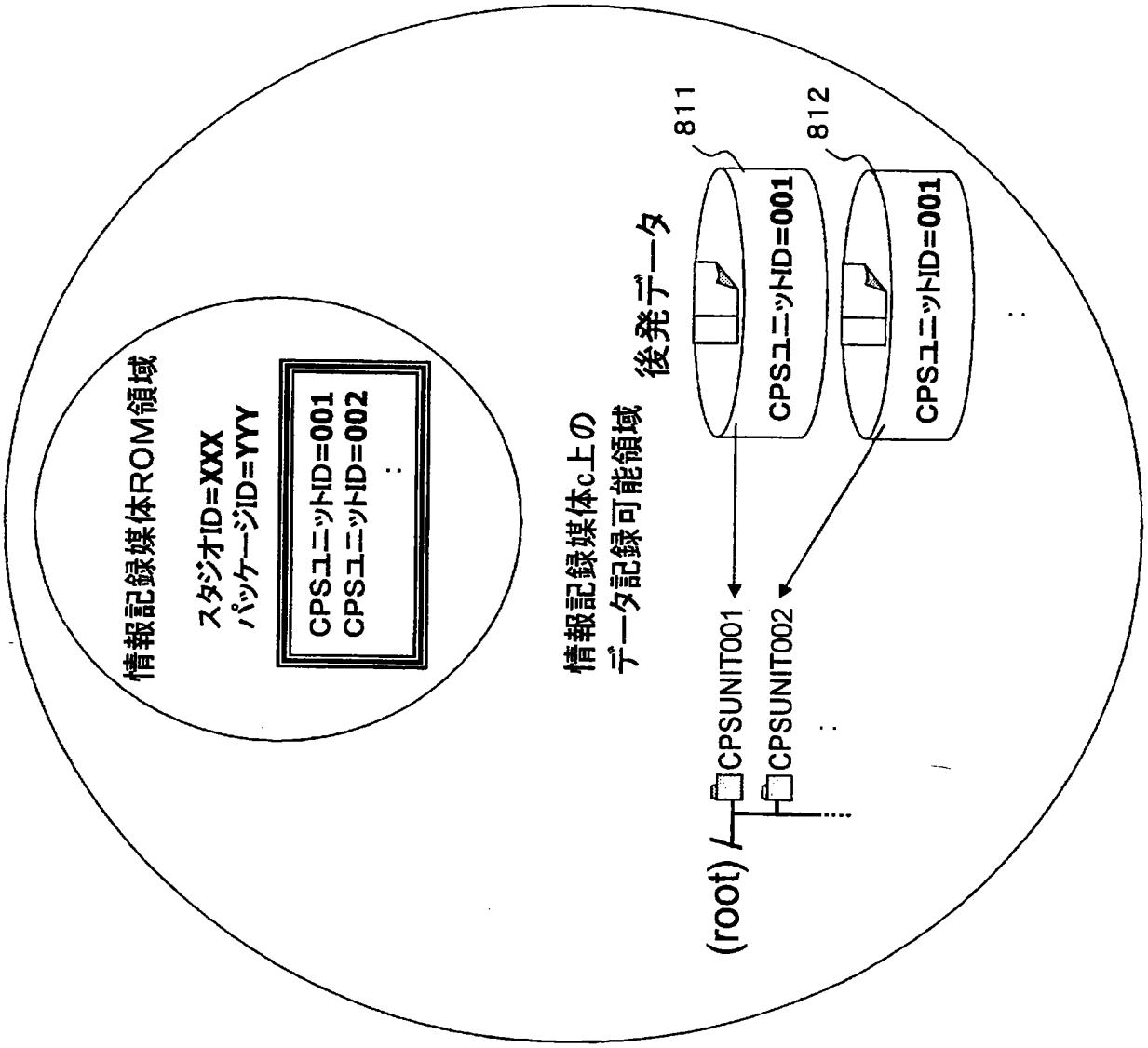
[図16]


803
記憶手段
後発データ
804
スタジオID=002
パッケージID=123
CPSユニットID=001
805
スタジオID=002
パッケージID=123
CPSユニットID=002
806
スタジオID=XXX
パッケージID=YYY
CPSユニットID=001
(root)
BDROM
STUDIO002
PACKAGE123
CPSUNIT001
CPSUNIT002
STUDIOXXX
PACKAGEYYY
CPSUNIT001
CPSUNIT002
関連付け
関連付け
801
情報記録媒体
スタジオID=002
パッケージID=123
CPSユニットID=001
CPSユニットID=002
802
情報記録媒体
スタジオID=XXX
パッケージID=YYY
CPSユニットID=001
CPSユニットID=002

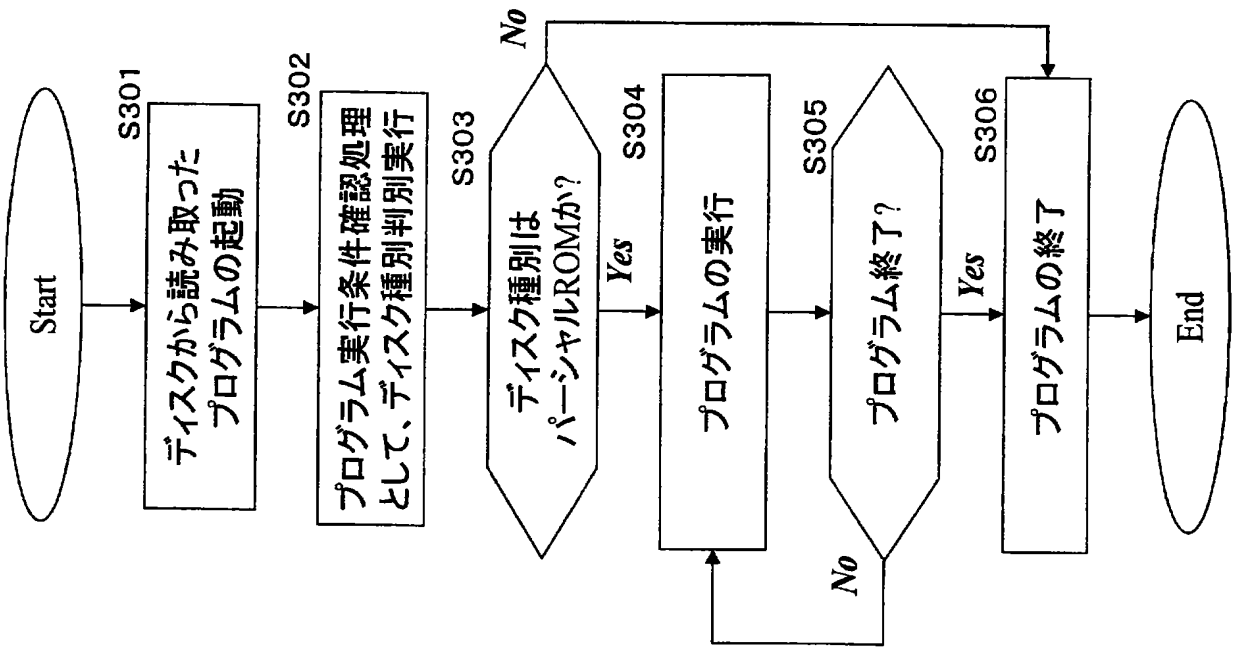
[図17]


記録先の名前空間を定義
<directoryName>：ディレクトリ名
<FileName>：ファイル名
Local Storage HDD
Local-HDD://
Local-HDD:// *(<directoryName>/)<fileName>
パーシャルROMの書き込み可能領域
Partial-ROM://
Partial-ROM:// *(<directoryName>/)<fileName>

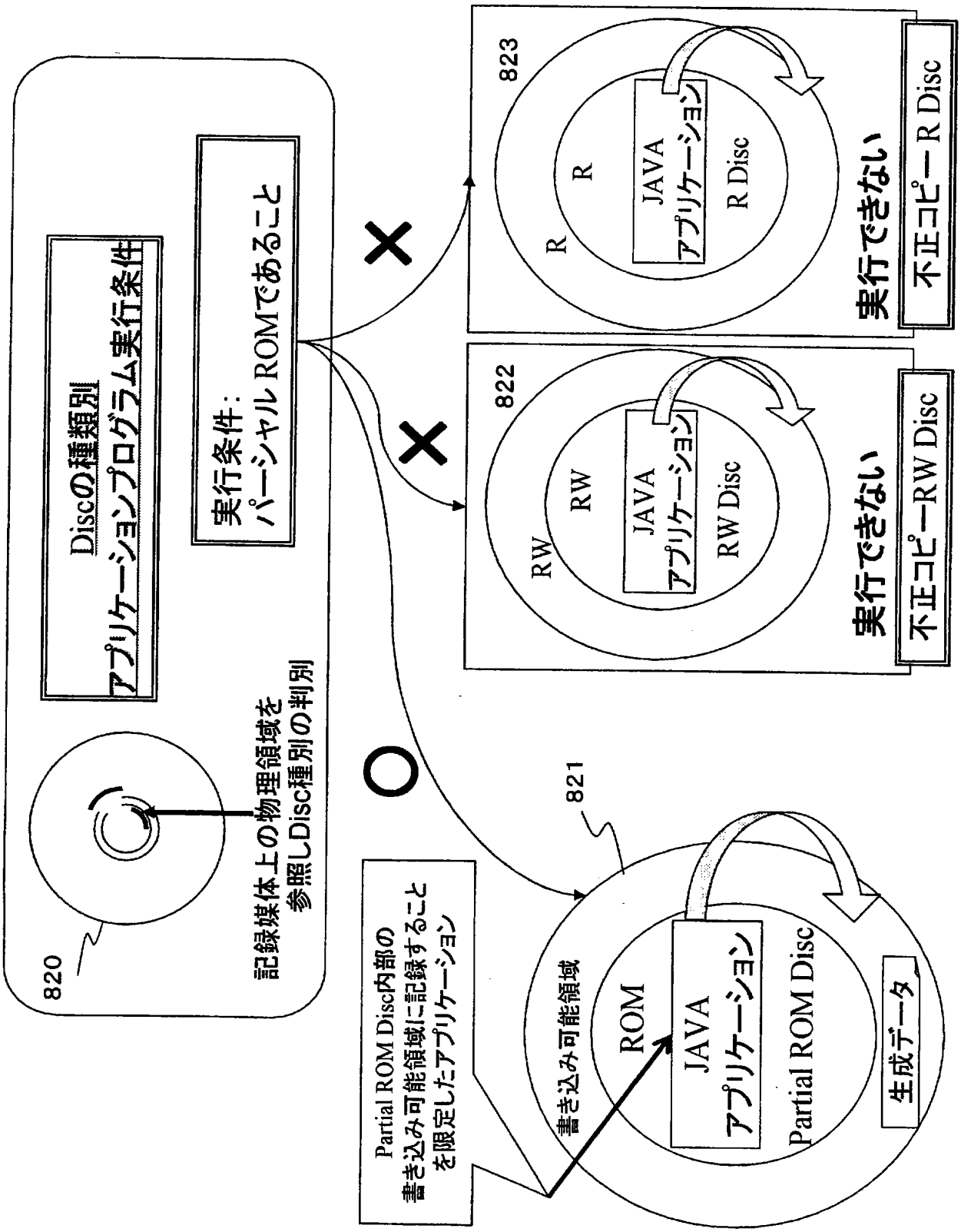
[図18]


情報記録媒体ROM領域
スタジオID=XXX
パッケージID=YYY
CPSユニットID=001
CPSユニットID=002
情報記録媒体c上の
データ記録可能領域
後発データ
811
812
CPSユニットID=001
CPSユニットID=001
(root)
CPSUNIT001
CPSUNIT002

[図19]

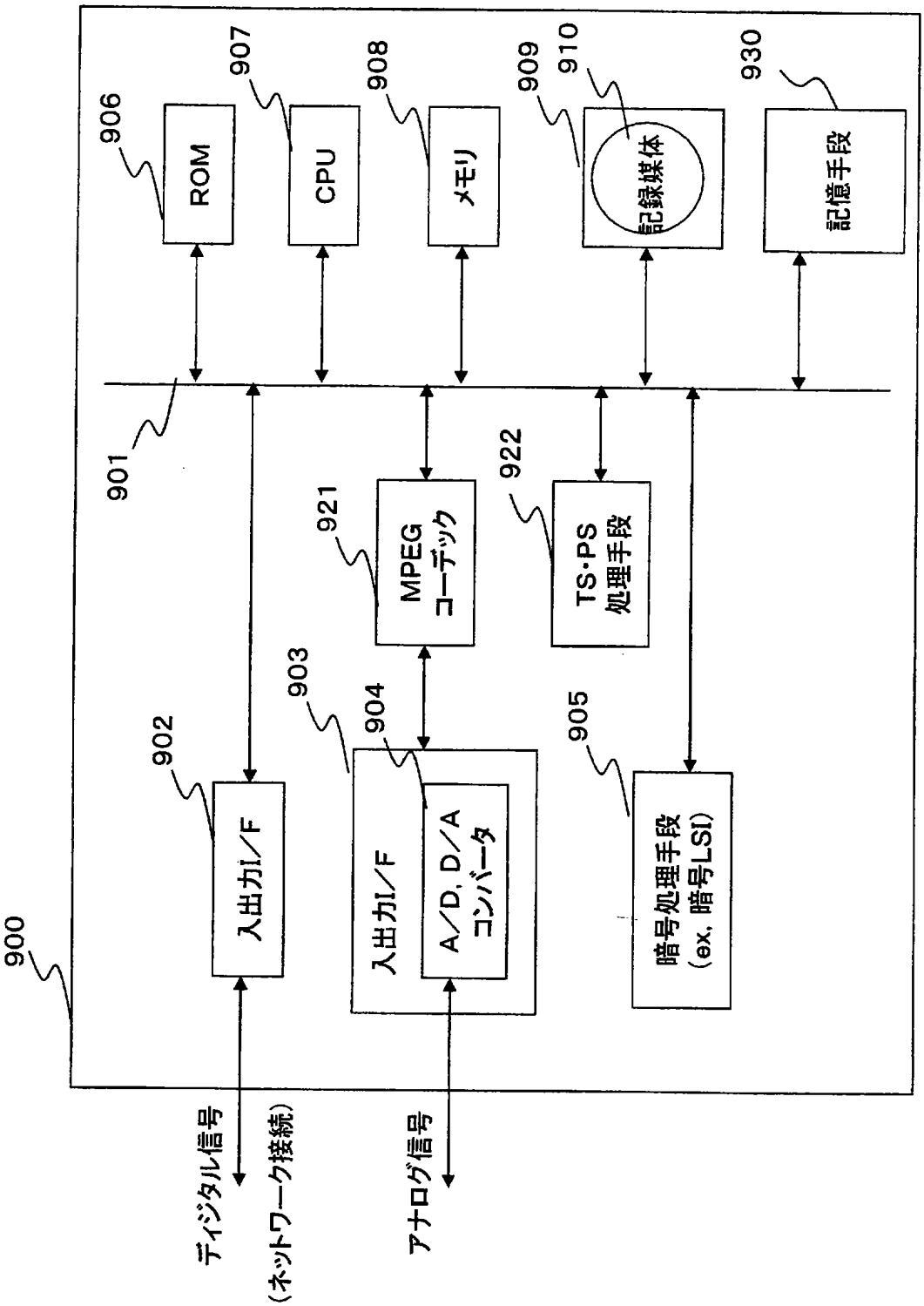

Start
S301
ディスクから読み取ったプログラムの起動
S302
プログラム実行条件確認処理として、ディスク種別判別実行
S303
ディスク種別はパーシャルROMか?
No
Yes
S304
プログラムの実行
S305
プログラム終了?
No
Yes
S306
プログラムの終了
End

[図20]


820
記録媒体上の物理領域を
参照しDisc種別の判別
Discの種類別
アプリケーションプログラム実行条件
実行条件:
パーシャルROMであること
Partial ROM Disc内部の
書き込み可能領域に記録すること
を限定したアプリケーション
821
書き込み可能領域
ROM
JAVA
アプリケーション
Partial ROM Disc
生成データ
822
RW
RW
JAVA
アプリケーション
RW Disc
実行できない
不正コピーRW Disc
823
R
R
JAVA
アプリケーション
R Disc
実行できない
不正コピーR Disc

WO 2005/074187 PCT/JP2005/001147

[図21]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/001147

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/10, G06F12/14, G09C1/00, G11B7/007, 7/30, 20/10, 20/12

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L9/10, G06F12/14, G09C1/00, G11B7/007, 7/30, 20/10, 20/12

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2005
Kokai Jitsuyo Shinan Koho	1971-2005	Toroku Jitsuyo Shinan Koho	1994-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2001-350664 A (Nippon Telegraph And Telephone Corp.), 21 December, 2001 (21.12.01), Par. Nos. [0038] to [0074] (Family: none)	1-13,16-28, 31-34
Y	"Joho Capsule Ryutsu ni Okeru Riyosha System Hogo", Information Processing Society of Japan Kenkyu Hokoku, Vol.2001, No.15, 20 February, 2001 (20.02.01), pages 103 to 108, particularly, 2.1 Joho Capsule to sono Ryutsu Framework, 3.3. Ninsho o Sansho	1-13,16-28, 31-34

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 April, 2005 (25.04.05)	17 May, 2005 (17.05.05)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/001147

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	"Juraigata Denshi Mall o Kakucho shita Online Contents Hanbai System", Information Processing Society of Japan Kenkyu Hokoku, Vol.99, No.11, 30 January, 1999 (30.01.99), pages 87 to 93, particularly, 4.3.1 Kenri Hogo Contents Kozo, 4.4.1 Secure Container Kozo o Sansho	1-13,16-28, 31-34
Y	JP 2001-209583 A (Sony Corp., Sony Computer Entertainment Inc.), 03 August, 2001 (03.08.01), Par. Nos. [0044] to [0063], [0517] to [0527], [0555], [0557] & WO 01/55858 A1 & AU 200128829 A & BR 200104213 A & EP 1195684 A1 & KR 2001109323 A & US 2002/154779 A1 & CN 136637 A & TW 1366637 A & MX 2001009394 A1	1-13,16-28, 31-34
Y	JP 2001-23299 A (ED-CONTRIVE INC.), 26 January, 2001 (26.01.01), Par. Nos. [0020] to [0022] (Family: none)	14,15,29,30, 35
Y	JP 2002-190157 A (Mitsubishi Electric Corp.), 05 July, 2002 (05.07.02), Par. Nos. [0019] to [0025] (Family: none)	14,15,29,30, 35
A	JP 2003-131949 A (Fujitsu Ltd.), 09 May, 2003 (09.05.03), Par. Nos. [0006] to [0009], [0014] to [0082]; particularly, Par. Nos. [0034] to [0037], [0050] & US 2003/084281 A1	1-13,16-28, 31-34
A	WO 2002-67125 A1 (DESIGN SITE ENTERTAINMENT PTY LTD), 20 February, 2002 (20.02.02), All pages & EP 134065 A1 & AU 2002242450 A1 & JP 2004-530241 A & US 2004/236588 A1	1-13,16-28, 31-34
A	JP 2001-325747 A (Mitsubishi Chemical Corp.), 22 November, 2001 (22.11.01), Par. Nos. [0202] to [0224] & WO 01/48753 A1 & AU 200122212 A & EP 1168322 A1 & US 2002/019948 A1 & US 2002/064111 A1	1-13,16-28, 31-34
A	"NGI Project (8) Contents no Capsule-Ka to Access Seigyo", UNIX MEGAZINE, Vol.15, No.9, 01 September, 2000 (01.09.00), pages 158 to 166, All pages	1-13,16-28, 31-34

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/001147

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. Claims 1-13, 16-28, 31-34
2. Claims 14, 15, 29, 30, 35

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☒ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

国際調査報告

国際出願番号 ＰＣＴ／ＪＰ２００５／００１１４７

A. 発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.[7] H04L9/10, G06F12/14, G09C1/00, G11B7/007, 7/30, 20/10, 20/12

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.[7] H04L9/10, G06F12/14, G09C1/00, G11B7/007, 7/30, 20/10, 20/12

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００５年
日本国実用新案登録公報	１９９６－２００５年
日本国登録実用新案公報	１９９４－２００５年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP 2001-350664 A （日本電信電話株式会社） 2001.12.21, 第38-74段落（ファミリなし）	1-13, 16-28, 31-34
Y	情報カプセル流通における利用者システム保護, 情報処理学会研究報告, Vol.2001, No.15, 2001.02.20, p.103-108 特に2.1 情報カプセルとその流通フレームワーク, 3.3 認証 を参照	1-13, 16-28, 31-34

☑ Ｃ欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー

「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの

「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「Ｏ」口頭による開示、使用、展示等に言及する文献

「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「＆」同一パテントファミリー文献

国際調査を完了した日 ２５．０４．２００５	国際調査報告の発送日 17.5.2005
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員） 5M 9364 中里　裕正 電話番号　０３－３５８１－１１０１　内線　３５９９

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（２００４年１月）

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ	従来型電子モールを拡張したオンラインコンテンツ販売システム， 情報処理学会研究報告，Vol. 99，No. 11，1999. 01. 30，p. 87-93 特に 4. 3. 1 権利保護コンテンツ構造，4. 4. 1 セキュアコンテナ構造 を参照	1-13, 16-28, 31-34
Ｙ	JP 2001-209583 A （ソニー株式会社，株式会社ソニー・コンピュータエンタテインメント） 2001. 08. 03, 第 44-63，517-527，555，557 段落 & WO 01/55858 A1 & AU 200128829 A & BR 200104213 A & EP 1195684 A1 & KR 2001109323 A & US 2002/154779 A1 & CN 136637 A & TW 1366637 A & MX 2001009394 A1	1-13, 16-28, 31-34
Ｙ	JP 2001-23299 A （イーディーコントライブ株式会社） 2001. 01. 26，第 20-22 段落（ファミリなし）	14, 15, 29, 30, 35
Ｙ	JP 2002-190157 A （三菱電機株式会社） 2002. 07. 05，第 19-25 段落（ファミリなし）	14, 15, 29, 30, 35
Ａ	JP 2003-131949 A （富士通株式会社） 2003. 05. 09，第 6-9，14-82 特に 34, 37, 50 段落 & US 2003/084281 A1	1-13, 16-28, 31-34
Ａ	WO 2002-67125 A1 (DESIGN SITE ENTERTAINMENT PTY LTD) 2002. 02. 20，全頁を参照 & EP 134065 A1 & AU 2002242450 A1 & JP 2004-530241 A & US 2004/236588 A1	1-13, 16-28, 31-34
Ａ	JP 2001-325747 A （三菱化学株式会社） 2001. 11. 22，第 202-224 段落 & WO 01/48753 A1 & AU 200122212 A & EP 1168322 A1 & US 2002/019948 A1 & US 2002/064111 A1	1-13, 16-28, 31-34
Ａ	ＮＧＩプロジェクト（８）コンテンツのカプセル化とアクセス制御， ＵＮＩＸ　ＭＡＧＡＺＩＮＥ，Vol. 15，No. 9，2000. 09. 01，p. 158-166 全頁 を参照	1-13, 16-28, 31-34

国際調査報告

国際出願番号 ＰＣＴ／ＪＰ２００５／００１１４７

第Ⅱ欄　請求の範囲の一部の調査ができないときの意見（第１ページの２の続き）

法第8条第3項（ＰＣＴ17条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1．☐ 請求の範囲＿＿＿＿＿＿＿＿＿＿ は、この国際調査機関が調査をすることを要しない対象に係るものである。
つまり、

2．☐ 請求の範囲＿＿＿＿＿＿＿＿＿＿ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、

3．☐ 請求の範囲＿＿＿＿＿＿＿＿＿＿ は、従属請求の範囲であってＰＣＴ規則6.4(a)の第２文及び第3文の規定に従って記載されていない。

第Ⅲ欄　発明の単一性が欠如しているときの意見（第１ページの３の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

本願の請求の範囲は、以下にあげる２群の発明に分けられ、単一性を満たしていない。

１．請求の範囲 1-13, 16-28, 31-34

２．請求の範囲 14, 15, 29, 30, 35

1．☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。

2．☑ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。

3．☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。

4．☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。

☐ 追加調査手数料の納付と共に出願人から異議申立てがなかった。